NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EXTENDING THE TACTICAL WIRELESS INTERNET IN SUPPORT OF USMC DISTRIBUTED OPERATIONS

by

Glen C. Henton
Justin R. Swick

September 2006

Thesis Co-Advisors: Carl Oros
Rex Buddenberg

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Extending the Tactical Wireless Internet in Support of USMC Distributed Operations		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Henton, Glen C. and Swick, Justin R.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Marine Corps Warfighting Lab (MCWL) Quantico, VA Marine Corps Tactical Systems Support Activity (MCTSSA) Camp Pendleton, CA		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

This thesis will research, examine, and propose a Tactical Wireless Network Infrastructure Concept of Operations in Support of Distributed Operations. Research and analysis will include the capabilities and performance characteristics of the 802.16 equipment currently implemented as part of the Marine Corps Tactical Command and Control Architecture in support of Operation Iraqi Freedom. Current Distributed Operations doctrinal capabilities will be compared to a proposed Concept of Operations that incorporates the most current state of the art wireless technologies to maximize both capability and interoperability.

The method for evaluation will incorporate COTS products and Marine Corps tactical communications devices installed and operated in both a laboratory setting as well as a tactical field environment. Key performance metrics captured include equipment throughput capacity, communications bandwidth, range and distance limitations, power consumption, communications security, and transmission security. Additional metrics evaluated include level of equipment operational complexity and degree of interoperability with current USMC command and control architecture.

14. SUBJECT TERMS 802.16, WIMAX, OFDM, COTS, WLAN, MESH, MANET, Tactical Internet, Distributed Operations, DO, Redline, INTER-4, Tacticomp			**15. NUMBER OF PAGES** 109
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EXTENDING THE TACTICAL WIRELESS INTERNET IN SUPPORT OF USMC DISTRIBUTED OPERATIONS

Glen C. Henton
Captain, United States Marine Corps
B.A., The Ohio State University, 1999

Justin R. Swick
Captain, United States Marine Corps
B.A., University of Minnesota, 1997

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN
INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2006**

Authors: Glen C. Henton

Justin R. Swick

Approved by: Carl Oros
Thesis Co-Advisor

Rex Buddenberg
Thesis Co-Advisor

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis will research, examine, and recommend technology solutions that provide the capability to extend the tactical internet to support the United States Marine Corps concept of Distributed Operations. Distributed Operations doctrinal capabilities will be compared to a proposed Concept of Operations that incorporates the most current state of the art wireless technologies to maximize both capability and interoperability. Specifically, research and analysis will focus on the capabilities and performance characteristics of the IEEE 802.16 equipment currently implemented as part of the Marine Corps tactical command and control architecture in support of Operation Iraqi Freedom, and provide a thorough evaluation of COTS wireless mesh technologies in providing the tactical internet access layer required to support Distributed Operations units. The research culminates with an integration of both of these technologies in a simulated employment of Distributed Operations units dispersed in tactical environment.

The method for evaluation will incorporate COTS products and Marine Corps tactical communications devices installed and operated in both a laboratory setting as well as a tactical field environment. Although the research captures key performance metrics such as throughput capacity and transmission range, the primary focus of effort centers on the needs of the Distributed Operations user by evaluating system performance and operational complexity in support of command and control requirements comprising voice, video, data, and situational awareness capabilities.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACRONYMS AND ABBREVIATIONS

AES	Advanced Encryption Standard
AO	Area of Operations
AODV	Add-hoc On-demand Distance Vector
AP	Access Point
ARP	Address Resolution Protocol
C2CE	Command and Control Compact Edition
C2PC	Command and Control Personal Computer
C4	Command, Control, Communications and Computers
COP	Common Operational Picture
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf
DARPA	Defense Advanced Research Projects Agency
DAMA	Demand Assigned Multiple Access
DC	Direct Current
DDACT	Dismounted Data Automated Communications Terminal
DO	Distributed Operations
DoD	Department of Defense
DSR	Dynamic Source Routing
EPLRS	Enhanced Position Location Reporting System
FBCB2	Force Battle Control, Brigade and Below
FDD	Frequency Division Duplex
GIG	Global Information Grid
GIGA Lab	Global Information Grid Applications and Operations Code Laboratory
GPS	Global Positioning System
HF	High Frequency
HMMWV	High Mobility Multi-Wheeled Vehicle
IEEE	Institute of Electrical and Electronics Engineers

IP	Internet Protocol
JTRS	Joint Tactical Radio System
Kpbs	Kilobits per second
LAN	Local Area Network
LOE	Limited Objective Experiment
LOS	Line of Sight
LFOC	Landing Force Operations Center
LPI/LPD	Low Probability of Intercept/Low Probability of Detection
LRV	Light Reconnaissance Vehicle
MAC	Media Access Control
MAGTF	Marine Air-Ground Task Force
MANET	Mobile Ad-hoc Network
Mbps	Megabits per second
MCTSSA	Marine Corps Tactical Systems Support Activity
MCWL	Marine Corps Warfighting Lab
MDACT	Mounted Data Automated Communications Terminal
MEA	Mesh Enabled Architecture
MMR	Micro-Mesh Router
NCW	Network Centric Warfare
NLOS	Non-Line of Sight
NSA	National Security Agency
NPS	Naval Postgraduate School
OFDM	Orthogonal Frequency Division Multiplexing
OIF	Operation Iraqi Freedom
OLSR	Optimized Link State Routing
OSI	Open Systems Interconnect
OTM	On-the-Move
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Data Assistant
PKI	Public Key Infrastructure

PtMtp	Point-to-Multipoint
Ptp	Point-to-Point
QAM	Quadrature Amplitude Modulation
QDMA	Quadrature Division Multiplex Access
QOS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
SCR	Single-Channel Radio
SPAWAR	Space and Naval Warfare Center
SINCGARS	Single-Channel Ground and Airborne Radio System
SIPRNET	Secure Internet Protocol Router Network
SNMP	Simple Network Management Protocol
SS	Subscriber Station
STAN	Surveillance, Targeting and Acquisition Network
STS	Soldier Tactical Software
TBRPF	Topology Dissemination Based on Reverse Path Forwarding
TDD	Time Division Duplex
T/E	Table of Equipment
THHR	Tactical Handheld Radio
TOC	Tactical Operations Center
TNT	Tactical Network Topology
UHF	Ultra High Frequency
USSOCOM	United States Special Operations Command
VAP	Virtual Access Point
VHF	Very High Frequency
VOIP	Voice Over Internet Protocol
WIMAX	Worldwide Interoperability for Microwave Access

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Glen Henton – First off, I would like to thank the Lord for all his blessings and gifts. I also want to thank my lovely wife, Lori, for all of her understanding and support. Without her, life wouldn't be as bright. Lastly, I want to thank my son, Lyle, for his energy and perspective on life, and for giving me a reason to smile during stressful times.

Justin Swick – To my sons Brandon and Austin, thanks for enduring this long period of separation while I dedicated my time to completing this research - I've missed you more than you can imagine. To my thesis partner and good friend, thank you for your initiative and devotion to our work throughout this past year. Lastly, to my loving wife, Christine, your understanding and willingness to fully support my efforts during this stressful time will forever remind me of your selflessness, your personal sacrifice, and your lasting devotion to me and our family.

The authors would like to extend a sincere thanks to both LtCol Carl Oros and Rex Buddenberg for their continued support and guidance in completing this project. Their wisdom, insight, and mentorship proved invaluable from the beginning, and their personal involvement and dedication to this research ensured our success.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

As the Department of Defense focuses on adapting military doctrine to meet the national security needs of current and future threats emerging from this highly volatile world political situation, the military supporting establishment must also adapt. Over the past decade, several DoD publications have highlighted and emphasized the need for change within the military ranks. Through such doctrine and publications as Network Centric Warfare, FORCE Net, Joint Vision 2010 and Joint Vision 2020, the services have become thoroughly indoctrinated into the tenets force transformation, information superiority, and the critical importance placed on interoperability.

These publications made clear their intent; the military must change the way it fights its wars. More specifically, the military must evolve and transform the armed forces command and control capability into a concept of operations that will maximize combat effectiveness by drastically improving the quantity and quality of information available to the warfighter. The primary means of achieving this goal lies in networking the sensors, shooters, and decision makers throughout the battlefield. This seamless network will maximize the real-time situational awareness capability for the warfighter, increase the decision-making efficiency of the commander, leverage greater lethality against the enemy, and minimize friendly casualties and collateral damage.

With every new conflict, our command and control capability continues to support the warfighter in more austere and demanding environments with an increased demand on information to and from the battlefield. During each new conflict, the individual warfighter relies more and more on increased command and control capability to support the mission. In addition to tactical voice communications, the maneuver elements now demand the capability to send and receive data communications, to include instant chat and video transmission. The expectation remains that these capabilities will extend down lower and lower into the organizational echelons, eventually reaching the individual soldier or Marine.

Currently, our command and control capability has reached its limits in providing these services. Our ability to fully support the traditional tactical architectures with adequate throughput and bandwidth also falls short, due in large part to the bandwidth bottlenecks created by legacy radios and the lack of integration between long-haul and tactical links. Numerous Army and Marine Corps units, from battalions to major subordinate commands, utilize commercial satellite and network services in support of their wartime operations. The smaller combat units – battalions and below - cannot take advantage of battlefield information superiority if they continue to operate while remaining digitally divided from their higher echelons. Particularly in support of the DO concept, the companies, platoons, squads, and even fire-teams must possess the capability to seamlessly communicate both vertically and laterally in conducting their operations. Current analog voice systems and equipment cannot support this requirement. Simply stated, Distributed Operations units - conducting missions in a widely-dispersed and autonomous manner - will require a command and control capability that exceeds current USMC fleet inventory. The Marine Corps must transform established command and control tactics, techniques and procedures to successfully support DO missions executed in the highly fluid and dynamic battlefields of the future.

This research focuses on supporting the DO warfighter in this new and uncertain environment. This thesis addresses current command and control shortcomings in supporting USMC Distributed Operations and researches the potential that commercial off-the-shelf (COTS) systems, devices and COTS-like technology possess in extending the tactical internet to fully support all DO command and control requirements. New and evolving technology will be examined that may provide the command and control to support the Distributed Operations units in conducting their mission.

This project initially began as joint effort with Space and Naval Warfare Systems Center (SPAWAR) San Diego with the intent to evaluate vendors and products as the SPAWAR contractual process developed. However, due to SPAWAR's project delays and subsequent loss of MCWL funding, the NPS project team was forced to conduct the

research alone and chose to use "best of breed" COTS products provided by INTER-4 and Redline Communications. A brief evaluation of these choices is provided in Appendix A.

B. OBJECTIVES

This research evaluates COTS and COTS-like mesh technologies and IEEE 802.16 standards-based wireless technology to determine whether they can provide the capability to support the command and control requirements of and extend the tactical internet to Distributed Operations units.

C. RESEARCH QUESTIONS

1. Can COTS and COTS-like wireless mesh and IEEE 802.16 broadband systems, devices, and technology extend the tactical internet to reach Distributed Operations units?

2. What advantages and disadvantages do wireless mesh and IEEE 802.16 technologies present to the Distributed Operations concept when compared to current command and control assets available to Distributed Operations units?

D. SCOPE

The scope of this thesis will include:

1. A review of the United States Marine Corps Distributed Operations concept along with the current command and control architecture available to support it as well as an overview of the proposed communications assets required to support Distributed Operations as identified by the Marine Corps Warfighting Lab.

2. A review of COTS and COTS-like wireless mesh technologies that can be leveraged to provide the tactical internet access layer[1] connectivity down to the Distributed Operations warfighter.

[1] The term "access layer" refers to a system and/or service that provides the end-user access to the network.

3. Laboratory and field experimentation to test COTS wireless mesh and IEEE 802.16 systems against the key performance metrics and applicability in providing the specific command and control capabilities to the Distributed Operations decision-makers.

E. METHODOLOGY

1. Research DoD and USMC publications and documentation for Distributed Operations concept of operations information and current and proposed command and control system and equipment requirements.

2. Research text books, related reference material, and industry experts pertaining to COTS wireless mesh networking and IEEE 802.16 wireless broadband technologies in order to obtain the required information to implement and analyze a meshed access layer network and an 802.16 battlefield backbone[2] link in support of a Distributed Operations field experiment.

3. Perform controlled tests and observe qualitative performance requirements to assess the wireless mesh and 802.16 technologies and provide relevant evaluation of the observed results.

F. ORGANIZATION OF THESIS

CHAPTER I. Introduction : This chapter identifies recent DoD initiatives addressing transformation and evolving command and control practices and procedures within the military establishment that precluded the creation of the Distributed Operations concept and discusses the challenges presented in supporting Distributed Operations and the reason for conducting this research.

CHAPTER II. Distributed Operations: This chapter presents an overview of the United States Marine Corps Distributed Operations concept. This chapter also provides a comparison of both the current communications inventory available to support the operations and the proposed command and control assets recommended by the Marine Corps Warfighting Lab to adequately support near-term Distributed Operations.

[2] The term "Battlefield Backbone" represents the part of the command and control system that serves as a long-haul communication link or provides the "reach-back" capability and has traditionally remained vehicular dependent.

CHAPTER III. Mesh Networks: This chapter provides an in-depth examination into the emerging technology of wireless meshed networks within the commercial sector. This chapter presents the pivotal technology that is employed during the experimental phase and reported in chapters IV and V.

CHAPTER IV. Experiment and Equipment Overview: This chapter highlights the vendor-specific COTS products that were implemented in support of the testing and experimentation during this research. These products provide a fully functional meshed network and long-haul network communications capability that served as the evaluation platform throughout this thesis.

CHAPTER V. Field Experimentation: This chapter outlines all laboratory and field experiments conducted during this research and provides detailed results of each test.

CHAPTER VI. Distributed Operations Architecture Considerations: This chapter highlights the recommendations developed as a result of the research conducted and experience gained during this experimentation.

CHAPTER VII. Conclusion and Recommendations for Further Research: This chapter provides a summary conclusion and recommendations for additional areas of research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. DISTRIBUTED OPERATIONS

A. DISTRIBUTED OPERATIONS CONCEPT

The concept of Distributed Operations (DO) developed as a result of the United States Marine Corps' initiative in transforming the way in which it will fight our nation's future battles. This concept, still in its infancy, seeks to maximize small unit maneuver warfare and effectiveness across a non-linear battlespace through the employment of responsive joint-fires and the use of a robust and seamless command and control communications backbone. DO will enable highly skilled small unit leaders to operate in widely dispersed and often-times autonomous environments. Furthermore, the Marine Corps Warfighting Lab (MCWL) identifies the Distributed Operations concept as "…an operating approach that seeks to create an advantage over an adversary – spatial, temporal, and psychological – through the intentional use of dispersion and independent, small-unit tactical actions, which are enabled by increased access to functional support." [1]

The Distributed Operations concept emphasizes dispersion and independent operation within its view of small unit tactical battlefield employment. The DO concept requires a robust, reliable, and efficient command and control capability while acknowledging the fact that disparate small unit missions will likely operate beyond the effective range of mutually supporting organic direct fires. The DO concept envisions these highly-trained small unit actions as promoting complementary capabilities, with the individual results combining to foster a much more profound effect than would otherwise prove attainable. These following tenets comprise the goals of DO, as defined by MCWL:

1. Develop a greater institutional commitment to the training of enlisted combat leaders.
2. Empower small units with enhanced capabilities; provide education and training to enable Marines to better accomplish the mission.

3. Provide Marines with the best equipment in the world and the training to employ it. [2]

Furthermore, Marine Corps General Mike Hagee, Commandant of the Marine Corps, summarized the concept of DO in one concise sentence, "Distributed Operations describes an operating approach that requires new ways to educate and train our Marines and that guides us in the use of emerging technologies."[3] This concept overwhelmingly emphasizes the potential impact that Marine Corps small unit leadership possesses in accomplishing a combat mission. The DO small unit leader, through maximum decentralization of informed decision-making and enhanced small unit combat capabilities, will provide an even greater maneuver warfare capability for the United States Marine Corps.

B. CURRENT DISTRIBUTED OPERATIONS COMMUNICATIONS EQUIPMENT AND CAPABILITY

In order to fully support the concept of DO on the battlefield the Marine Corps must look beyond the current equipment inventory. Current Table of Equipment (T/E) allowance for an infantry platoon includes only one VHF radio. The primary radio filling this role remains the AN/PRC-119a/b/f variant of the Single Channel Ground and Airborne Radio System (SINCGARS) series of tactical VHF radios. Beyond this asset addressed formally within the T/E, only the Personal Role Radio (PRR) extends farther down the unit echelons to reach the squad and fire-team units, albeit with a very limited range and capability. Figure 1 provides an overview of current Marine Corps T/E allowance as applied to a DO company and below.

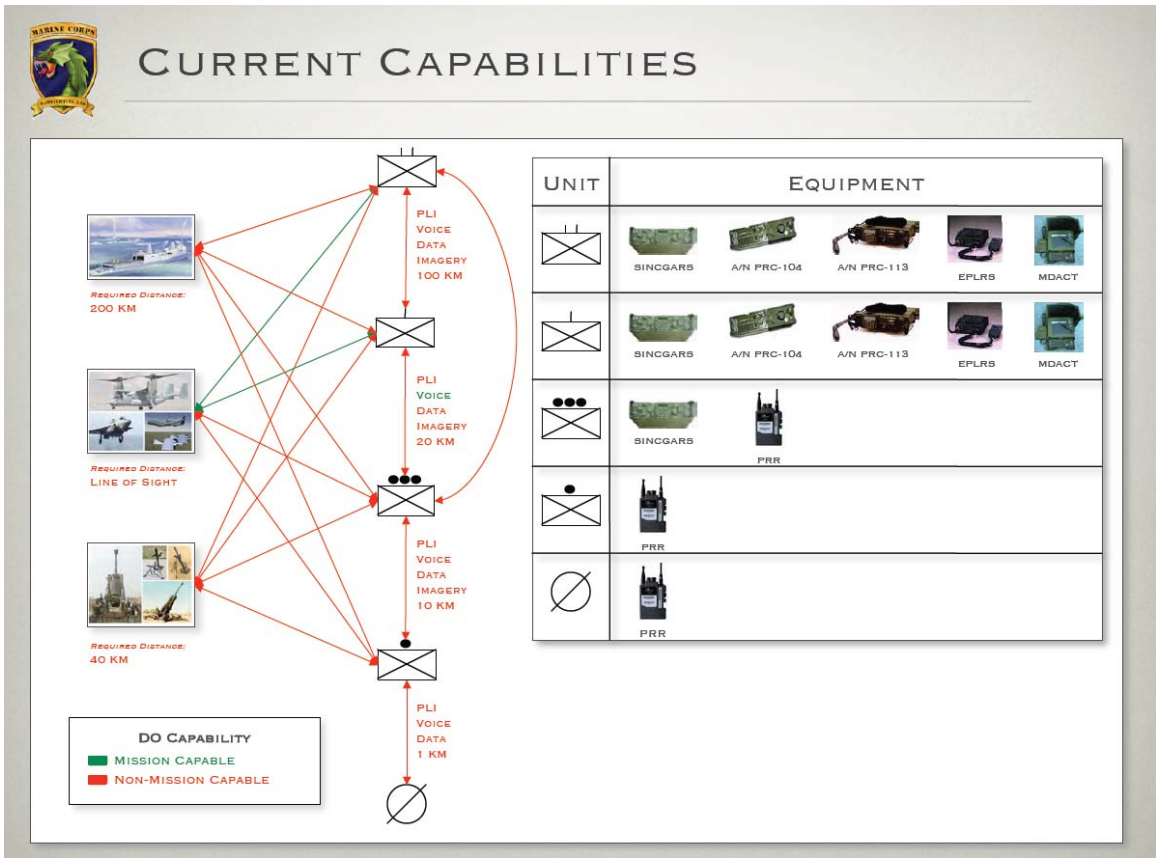

Figure 1. Current T/E Supporting the Infantry Company and Below (From: [2])

As depicted in Figure 1, virtually all capabilities required by DO units remain unsupportable. Even though SINCGARS has successfully supported the U.S. military in providing reliable voice communication across the battlefield, this equipment neither possesses the required range nor adequately transmits data needed to support the concept of DO, much less possess the ability to adapt into any form or likeness of a networked battle space. Unfortunately, SINCGARS is not alone in its inability to pass data at a satisfactory rate. The burden of legacy radio systems such as SINCGARS on current operations is readily apparent in today's battlefield. Table 1 below highlights the results of the U.S. Army's research into bandwidth constraints and identifies not only the poor data transmission capability of the SINCGARS radio but also that of several other legacy

USMC T/E communications systems to include the Enhanced Position Location Reporting System (EPLRS) and the primary terrestrial satellite communications platforms found within the Marine Corps as well as the U.S. Army.

Maximum Engineering and Effective Bandwidth for Typical Army Communications Equipment in 2003

(In kilobits per second)

Radio/Communications Equipment[a]	Typical Battlefield Command Levels	Point-to-Point Data Throughputs	
		Maximum Engineering	Average Effective[b]
SINCGARS (SIP)	Vehicle to Corps	16	1.7
EPLRS (VHSIC)	Company to Corps	128	13.3
NTDR	Company to Corps	288	30
Interface Standard[c]	Battalion to Army	16	1.5 to 7
MSE	Battalion to Corps	64	1.7
MSE with ATM Switch	Brigade to Corps	2,048[d]	5.1 to 6.7
DSCS-111/93	Division to Army	256	27[e]
DSCS-111/85	Division to Army	768	82[e]
SMART-T	Brigade to Army	4,620	481[e]
STAR-T[f]	Corps to NCA[g]	24,000	2,500[e]

Source: Congressional Budget Office based on the Army's 1999 budget hearing for its command, control, communications, and computer (C4) systems.

a. See the **glossary of abbreviations**.

b. These averages are lower than the maximum engineering throughputs because of the bandwidth required for context bits and channelization. The averages apply until about 2007, when the Army will begin to field the initial examples of a new generation of communications equipment (see **Chapter 2** and **Appendix A** for more details). After a transition period between 2007 and 2010, Objective Force units in 2010 are scheduled to be the first units to incorporate the new equipment in its entirety.

c. Used for multiplexers, modems, routers, switches, radio access units, and other equipment.

d. The maximum potential rate is 8.192 megabits per second using the (high-capacity line-of-sight) HCLOS radio--provided the interfaces are programmed to operate at the higher rates and frequencies are available. However, at present, the interfaces are not so programmed.

e. Extrapolated from the reductions in bandwidth that occur for lower-frequency radios.

f. The termination in 2001 (for default, as a result of delays and cost overruns) of the ongoing contract for the STAR-T has cast doubt on the program's future. To fill the void produced by the termination, the Army is currently using commercially available systems of approximately the required throughputs and considering replacement candidates.

g. The NCA, or National Command Authority, refers to the command chain that extends to the Secretary of Defense and the President.

Table 1. Effective Throughput in Kilobits per Second (From: [4])

C. NEAR-TERM DISTRIBUTED OPERATIONS COMMUNICATIONS EQUIPMENT AND CAPABILITY

Over the next two years, the fielding of new generation legacy radio systems throughout the USMC operating forces will serve to only marginally enhance the data transmission capability from a tactical environment. As illustrated in Figure 2, several radio systems will be fielded over the next several years to include the Command and Control On-the-Move Network, Digital Over-the-Horizon Relay (CONDOR) Gateway, the AN/PRC-150 HF radio, the AN/PRC-117 Multi-band VHF/UHF radio, the AN/PRC-148 Multi-Band Inter/Intra Team Radio (MBITR), and the Integrated Intra Squad Radio. Several of these procurements will not be complete until 2011, and still fail to provide any significant capability enhancements in the transmission of data as compared to that of current inventory.

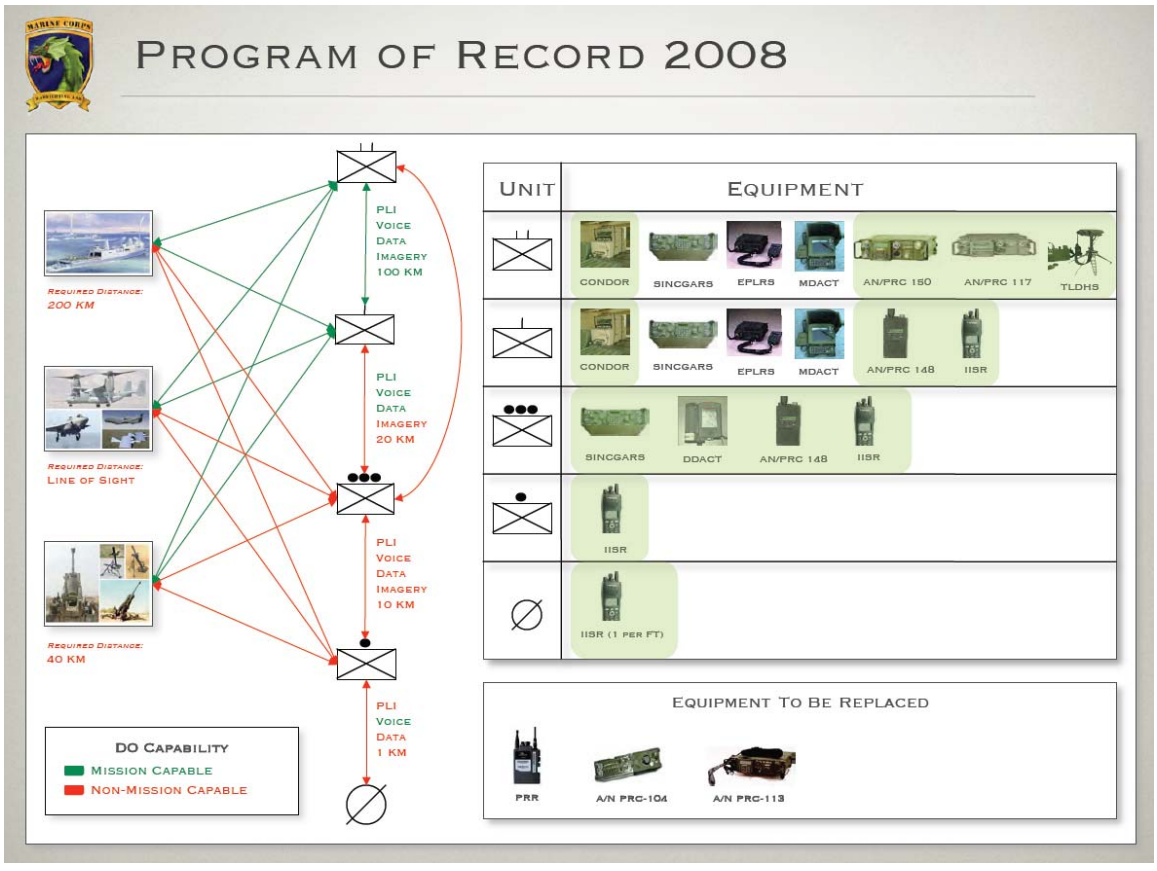

Figure 2. FY08 DO Table of Equipment (T/E) (From: [2])

D. PROPOSED DISTRIBUTED OPERATIONS COMMUNICATIONS EQUIPMENT AND CAPABILITY

In proposing a solution that provides all the capabilities required to support the DO concept, MCWL suggests outfitting all DO units with a netted low earth orbit satellite communication-enabled (LEO-SAT) Personal Digital Assistant (PDA). MCWL further suggests that the acquisition of this device could supplant several legacy radio systems and outdated data devices, namely the mounted and dismounted versions of the Digital Automated Communications Terminal (M-DACT and D-DACT), as highlighted in Figure 3 below.

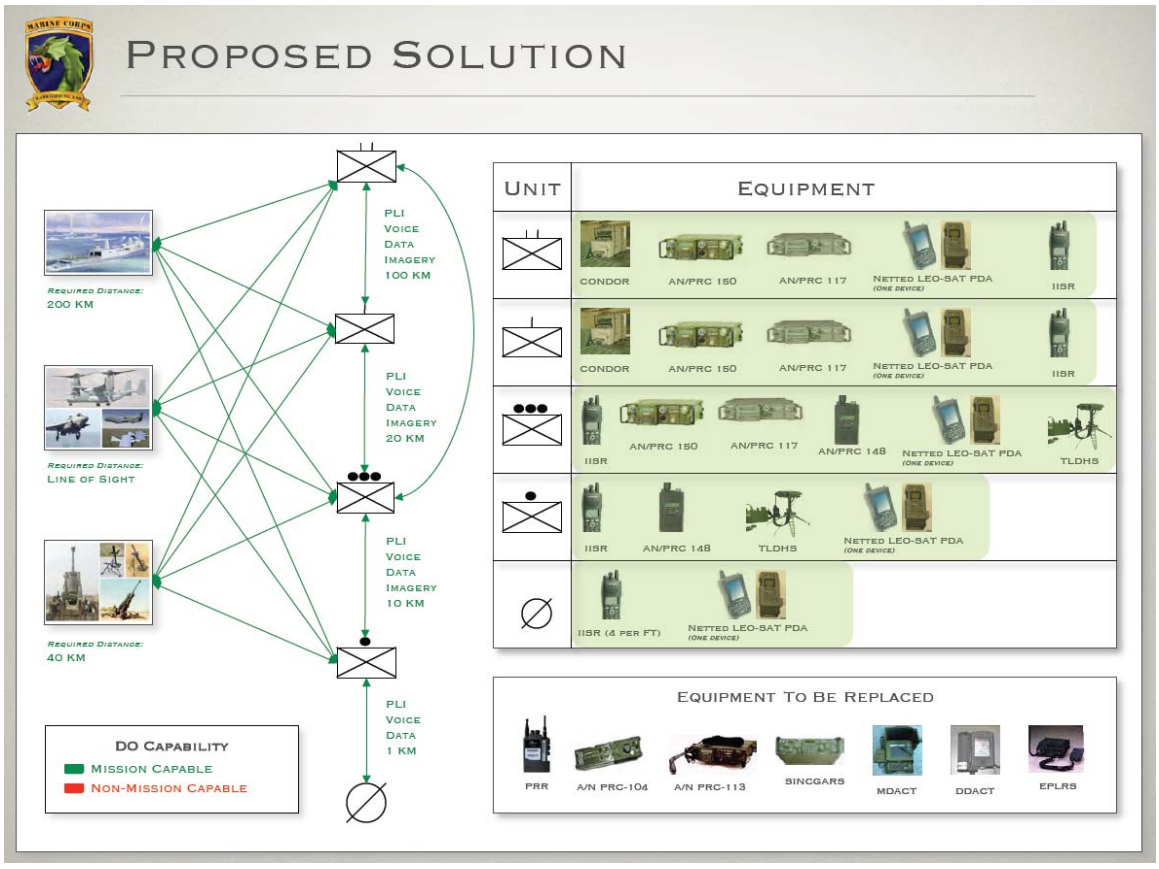

Figure 3. MCWL Proposed Solution (From: [2])

While an experimental LEO-SAT based communications device currently exists and continues to undergo initial testing, limited satellite communications channels, the

inability to multi-cast, and the lack of point-to-multipoint capability all remain a significant factor. This device, named the Experimental Tactical Communications System (ETCS), communicates via the Iridium satellite constellation, a purely narrowband point-to-point transmission system. Initially designed to support voice communication, the standard Iridium voice channel operates at only 8 kbps throughput capacity and cannot support more than one user per channel. Similar to the challenges that confront our legacy radio systems, this LEO-SAT alternative simply does not possess the transmission throughput capability to support timely imagery and streaming video transmissions and therefore remains ill-suited to support future DO missions.

The DoD's Joint Tactical Radio System (JTRS) family of software programmable radios initially held much promise for delivering a product that could provide a broadband battlefield backbone capability, as well as provide a wireless networking waveform to support highly mobile networked users. This program, initially conceived to serve as a centerpiece of US military transformation, has experienced significant cost, schedule, and performance delays over the past two years. The JTRS program experienced a major restructuring during the second quarter of fiscal year 2006, and will now design and build its family of radios in 4 increments instead of six clusters in a scaled-back and more limited acquisition initiative.

The JTRS primary waveform[3] supporting increment 1 will remain the same as before the restructuring. This waveform, called the Wideband Networking Waveform (WNW), provides JTRS with a general purpose tactical wireless access layer and battlefield backbone capability through the use of the same technology employed in both applications. This waveform technology, however, achieves only a fraction of the capability that IEEE 802.16 (2004) and IEEE 802.16e technologies possess. The WNW

[3] According to SPAWAR's JPEO JTRS web-site, a waveform is the entire set of radio and/or communications functions that occur from the user input to the radio frequency output and vice versa. JTRS waveform implementation consists of a Waveform Application Code, Radio Set Devices and Radio System Applications. Originally, there were 32 JTRS waveforms which have since been reduced to the following 9: WNW, Soldier Radio Waveform (SRW), Joint Airborne Networking-Tactical Edge (JAN-TE), Mobile User Objective System (MUOS), SINCGARS, Link-16, EPLRS, HF, and UHF SATCOM.

supports a 6.2-mile range with data transmit rates up 5 megabits/sec, while the IEEE 802.16 links tested within this research obtain ranges and throughput capabilities of over 5 times these figures.[4]

In order to fully support the capability to send and receive text data, still imagery data, voice, PLI, and streaming video, selected COTS and emerging wireless and broadband back-haul technologies must be researched and investigated for potential incorporation into future DO employment doctrine and capabilities matrices. Wideband, network-capable communications systems must replace current legacy narrowband offerings. In the following chapters, selected wireless mesh and IEEE 802.16 technologies are researched and evaluated in their ability to extend the tactical internet to reach DO units.

[4] See Chapter V, Figure 29 and Figure 30 for 802.16 throughput test results and selected range examples observed during the experimentation.

III. MESH NETWORKS

A. DISCUSSION OF MESH NETWORKS

Communication in a military environment is difficult due to its dynamic nature, changing environment, and lack of fixed infrastructure associated with wired connections. Due to these challenges, the military employs devices that transmit and receive information using the radio frequency (RF) spectrum. By using the RF medium, a military node (simply a communications device that is transported by a military member) is able to move about the battlefield free from the connections required in a wired environment. Consequently, the military is able to freely extend the distance between communicating nodes without the need for a wired connection.

For several decades the military has used radio devices to transmit and receive information that primarily consisted of analog voice data. This method provided a much-needed conduit to transmit and receive information, but the information that traveled through the connection was limited. These connections were limited to single channel radio and circuit switched phone networks. Now with the advent of Network Centric Warfare and the Internet, there is a need for these military radio devices to transmit and receive digital data that may consist of text, streaming video, voice, images, map graphics, etc., to multiple users dispersed on the battlefield. The process of getting the information from high-level Command Posts to mobile users on the battlefield is bridging the last tactical mile.

The means to inter-connect these military users that utilize the RF medium to disseminate digital information has been loosely termed mesh networking. Mesh networks merge routable, wireless devices to provide enhanced functionality for the military user. Mesh networking holds the promise to provide military nodes the ability to send and receive many different types of information (voice, digital data, imagery, streaming video, etc.) on the battlefield even if a military user lacks a direct connection to the originating node that sent the information. Each node in the network must have the

ability to forward information through the network until it arrives at the destination. In this example the mesh description is very simplistic, but in reality, the technologies that enable mesh are very complex.

There are specific reasons for mesh use in military applications. One of the reasons has been identified: a need for a communications medium that is not reliant upon fixed infrastructure and wired connections. Another reason is that military nodes operate in a dynamic environment and nodes may enter and leave at random intervals. Hence the mesh network needs to be self-forming and self-healing, that is the nodes can enter and leave without destroying the network. The network will simply adjust to the additions and subtractions. One last reason for mesh employment is military networks operate in environments that interfere with RF signals (mountains, foliage, buildings, etc.). Subsequently, the network must be able to adapt and find routes through the network in spite of these obstructions.

This chapter will describe the basic principles of mesh networking and the approaches that are needed for a functional and reliable mesh network.

B. MESH NETWORKS DEFINED

Many of the terms in this chapter come from Gilbert Held's book titled *Wireless Mesh Networks*. After researching many sources for useful and accepted mesh network descriptions, his book seems to have done the best job of breaking down the components of mesh networks in the simplest and most useful terms.

In order to develop a better understanding of how mesh networks are formed, the basic components of mesh networks must be defined. For this thesis, mesh networks are defined as: For *n* nodes in a network, where the term "node" refers to a communications device that can transport data from one of its interfaces to another, then the ability of each node to forward information for every other node in the network represents a mesh network topology. [5] A mesh network has the ability to forward information across successive daisy-chained nodes that are members of the network.

1. Nodes

As was previously referenced, a node, or communications station, is the lowest level of the mesh network. A node in the military environment is described as a

communications device that can transmit and receive data through an interface—in this scenario a radio interface. A node may consist of a communications device in a tank, an airframe, a Light Armored Vehicle, a HMMWV, or an individual dismounted Marine. A node is platform independent.

2. Link

In order to form a network, one or more nodes must form a connection with another node through the communications medium. This connection is called a link and there are three basic types. The connection between two nodes is called a point-to-point (Ptp) link and is illustrated in Figure 4. Another type of connection is a point-to-multipoint (PtMpt) link and is illustrated in Figure 5. Mesh networks use a third type of connection which is a series of Ptp connections, or point-to-consecutive-point links (see Figure 6). As will be described, mesh networks are at the same time flexible and complex.

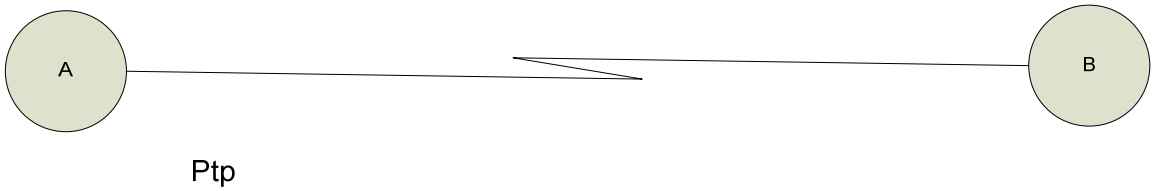

Figure 4. Point-to-Point Link

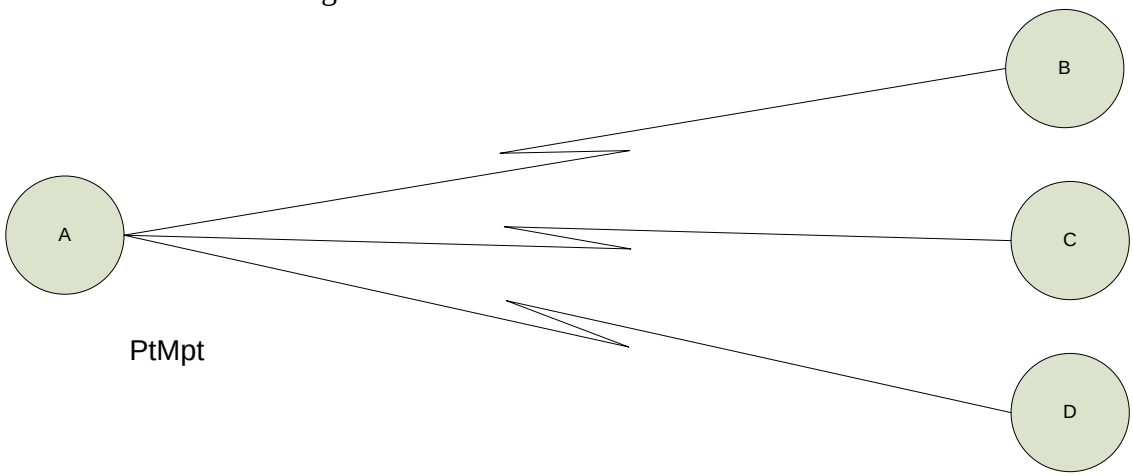

Figure 5. Point-to-Multipoint Link

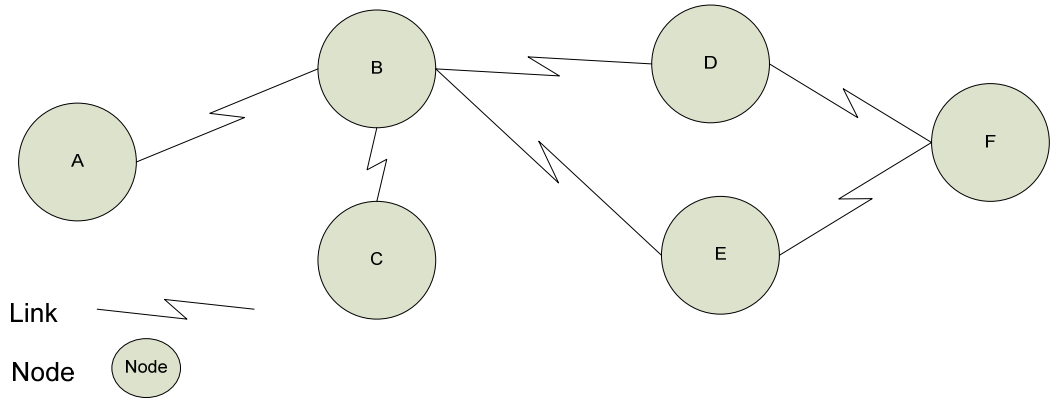

Figure 6. Simple Mesh Network

A link is formed when the two nodes are close enough in proximity to receive the other station's signals. When multiple nodes create connections and have the ability to transmit information through the entire network, a mesh network is created. In a properly built mesh network, a node has the ability to transmit or forward information for any node in the network regardless if that node has an established link to the originator or destination. In Figure 6, Node A has the ability to transmit information to Node F despite the fact it does not share a direct communication link with Node F. The series of connections through the network give the nodes the ability to forward information. The ability to traverse the network and extend the communications range is what makes a mesh network so flexible.

Despite the increased flexibility, mesh networks also provide increased complexity. In a network with N number of nodes, there is the potential that each node can communicate with every other node in the network. As N increases, the possibility for a greater number of links increases, and the more complex the network is to manage. Theoretically at some point, as N grows, the network will become unmanageable.

3. Forwarding Function

In addition to every node acting as a radio transmitter and receiver, each node must also function as a forwarding agent for the mesh network to function. The forwarding function appears simple in theory but in practice is quite difficult especially in large, dynamic mesh networks. For mesh networks to function, each node must develop

some form of a forwarding table, which is a map of the network. Without this map, a node will not have the ability to forward messages beyond a directly connected node.

Nodes develop this map, or view of the network, utilizing a discovery process. There are many ways for a node to map the network; a general description is all that is described here. Generally, a node discovers its directly connected neighbors and stores information about these nodes in a state table. The next step is for directly connected nodes to share the information in their state tables. After several iterations, convergence, or knowledge of the network, will be achieved. This information is then used to move information from one edge of the network to the other.

4. Self Forming/Self-Healing

Another key requirement for a mesh network in a military environment is the ability for nodes to enter and leave without disrupting the network. This process is defined in mesh terms as self-forming and self-healing. The military environment is a dynamic environment with vehicles, airframes, and personnel moving in and out of the battle-space at different intervals. The vision of mesh requires that the network should continue to function as nodes enter and leave with minimal disruption to the network. For this to occur, the information about the updated state of the network must be communicated and maintained in the nodes. This updated information keeps the network functioning.

5. Addressing

In order for the system to function and for nodes to be able to send and receive information, each node in the network needs an address for identification. Nodes are addressed with a unicast—or individual—address at two different layers in the OSI model. There are addresses for layer 2, which is the data link layer, and for layer 3, which is the network layer. The layer 2 address is the Media Access Control (MAC) address of the node's network interface. At layer 3 an internet protocol (IP) address is used. Multiple addresses may seem redundant, but each address is used for different purposes and enhances the functionality of the network.

In addition to a unicast address for each station, the network will also use a broadcast address for various purposes. The broadcast address is used to send

information or packets to every node in the network. The reason for a broadcast address is for simplicity. One broadcast address is used to send information to every station in lieu of addressing each node individually. The broadcast address is used by both layers 2 and 3 in the OSI model. Generally, the broadcast address is specified with all 1's, which implies that every bit in the address field is turned on. At layer 2 the address field consists of a 48-bit MAC address, and for broadcast purposes the field would display all F's (an example MAC broadcast address is FF-FF-FF-FF-FF-FF). Broadcast addressing is also used at layer 3 and a broadcast message is addressed with all 1's in the host portion of the 32-bit IP address field. For instance, a broadcast address for a Class B IP address would be X.X.255.255.

Another addressing scheme used in mesh networks is called multicast addressing. This addressing scheme also functions at layer 3 in the OSI model. Multicast addressing is similar to a broadcast address. In multicast, however, not every node in the network will receive the multicast message. The only nodes that will receive the multicast message are those nodes that subscribe to the multicast broadcast. As in a broadcast message, the multicast addressing targets many different nodes with one address and is less complicated than addressing the message to every node that subscribe to the broadcast.

6. Types of Nodes

There are multiple node types that may comprise the mesh network. These nodes are labeled as fixed, nomadic, and mobile nodes. Fixed nodes, as the name implies, do not move. This type of node simplifies network management because once the nodes enter the network, their information and connections to other devices will not change.

Nomadic nodes, on the other hand, will move periodically. Generally nomadic nodes will move from one location to another but will not require connectivity to the network while in transit. Once the nomadic node reaches its final destination, the node will re-enter the network and the new information about this node will eventually filter through the network via broadcast updates until network convergence is complete. The network's handling of these types of nodes is more complex than the handling for fixed nodes.

The type of node that is most difficult for the network to manage is the mobile node. A mobile node has the ability to move through the battle-space and requires a network connection during transit. This is a challenging event because the RF medium has physical limitations. An RF signal cannot propagate through the atmosphere indefinitely, and eventually a node will move beyond the RF range—or footprint—of its directly connected node. When this occurs, the mobile node will establish another link connection with a new node within RF range. The updated information will then be broadcast through the network. This step may repeat often depending on the speed of the mobile node and the RF distances between potential nodes. This is the most difficult scenario for the mesh network to manage.

C DATA LINK LAYER FUNCTIONS

The data link control layer manages all crucial functions that enable mesh networking. There are a number of different layer 2 technologies that can implement mesh network formation. The IEEE 802.16-2004 standard, the IEEE 802.16e standard, the yet to be approved IEEE 802.11s standard, the IEEE 802.15.4 ZigBee standard, and Motorola's ITT MEA mesh technology, which is based upon Quadrature Division Multiple Access (QDMA), are all layer 2 technologies that implement mesh. Each of these technologies functions differently and only layer 2 basic functions will be described here.

1. Network Entry/Exit

A layer 2 function is required to control and manage the entry and exit of multiple nodes in the network. Before a node enters the network, it must request to join the network. The term candidate node describes a node before it enters the network. The candidate node will send a network entry request to the node controlling the network. If the candidate does not have a direct connection to the controlling node, then it must send the request through a sponsor node that will in turn forward the request to the controlling node. Part of this process entails verifying whether a node has permission to enter the network (the authentication process will be described later). If the candidate node is successful it will become part of the network.

Network exit is another function that must be managed. In most layer 2 mesh technologies a node will not send a network exit request. Instead, the node will just move beyond the range of any network nodes and will not have the ability to communicate. Directly connected nodes will periodically send control messages to verify the status of the connection. After a node exits the network, it will not be able to return the control messages and the other nodes will determine it left the network. The updated information will then be broadcast through the network.

2. Scheduling

In order to minimize collisions in the network, a scheduling service must manage the number of nodes in the network and schedule the time for the devices to communicate. The controlling node will use the network map as a guide to build the transmission schedule. After the controlling node builds a schedule, it will send out a broadcast message to the network to specify the transmission schedule. Once the schedule is downloaded to the individual nodes, each node will use that schedule as a guide before transmitting.

Quality of service (QoS) information has become more important in today's networked environments. Certain types of data need higher prioritization in networks with high volumes of traffic. Because of the time-sensitive nature of streaming video, voice traffic, and video teleconferencing, this data should get a higher priority than e-mail or web traffic. QoS allows for this prioritization and provides more timely service to higher priority traffic. In some standards like 802.16, QoS information is used as input for building the schedule. The controlling node will poll the network nodes for QoS information and will use that information to determine the transmission schedule.

3. Mesh Network Frame Forwarding[5]

Mesh networks are capable of forwarding frames from one node in the network to another node regardless of the number of hops from the originating node. The process of forwarding frames across the network occurs solely at layer 2. Forwarding information—node MAC addresses and destination path information—for mesh networks is kept at the Logical Link Control (LLC) layer. Before a node sends information across

[5] The following information is based on the ITT mesh card's mode of operation. The ITT mesh card is described further in Chapter IV.

the network, the node will retrieve the forwarding information from the LLC layer and use that information to forward the frame through the network. Several peer-to-peer connections will be made in order for the frame to transit from the originating node to the destination. The LLC layer will constantly update its forwarding table as network changes are disseminated.

4. Handoffs

One of the most complex functions that must be managed at layer 2 deals with mobile nodes. As described earlier, mobile nodes require network service while moving through the battle-space and must be managed. At some point the mobile node will require a new connection with another node before it leaves the RF footprint of an established communication link. This transition is called a handoff. The best model of this process is a commuter driving down the road while talking on a cell phone and maintaining the connection even as the phone transitions from one cell phone tower to another. Figure 7 shows a depiction of the handoff process. As node C travels from left to right, it will eventually go out of range of node A. The handoff will occur when node C establishes a new connection to node B, and will provide uninterrupted connectivity. If the handoff fails or is delayed, node C will lose network connectivity.

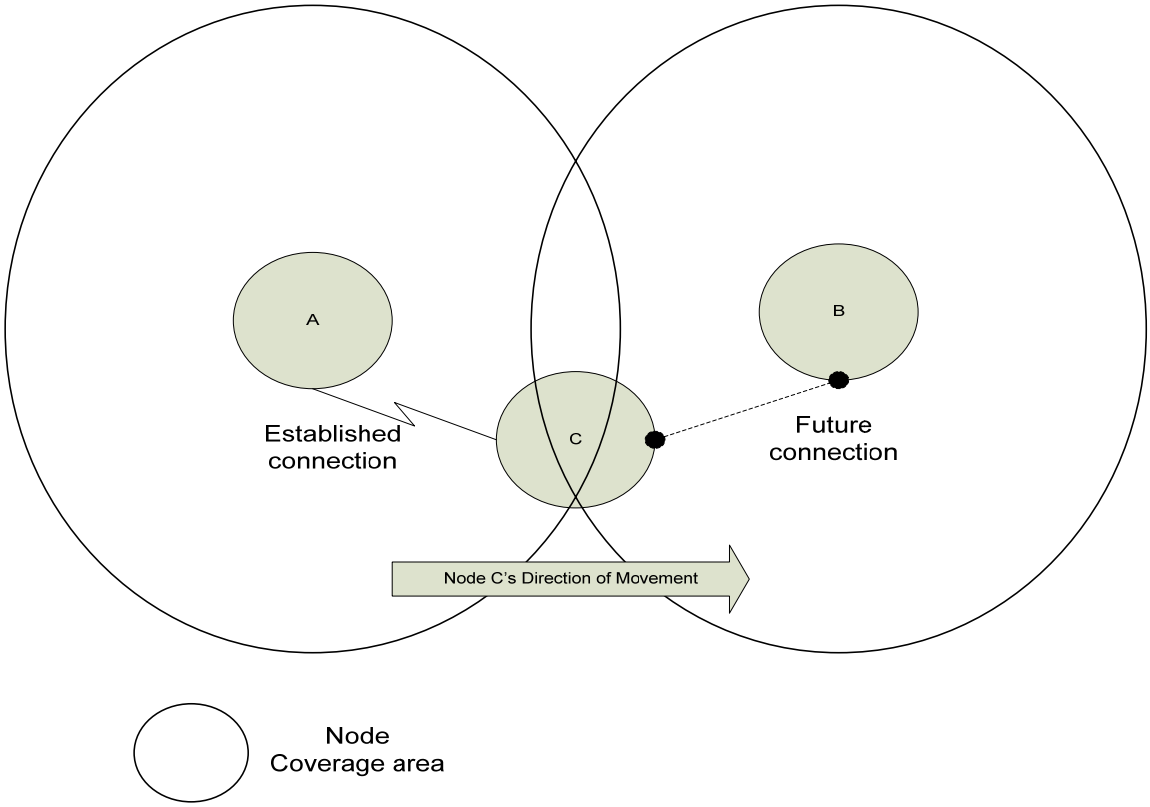

Figure 7. Hand-off with a Mobile Node

There are two types of handoffs, a soft handoff and a hard handoff. In a soft handoff, the process of forming a new link connection to another node is performed prior to tearing down the old link. The updated information is then quickly broadcast through the network and the node will continue to receive service. This is a smoother process and is the most preferred. Conversely, a hard handoff is more complex. A hard handoff occurs when the mobile node moves beyond its connection to the network prior to forming a new connection. In this instance, the mobile node will lose its network connection temporarily until it can establish another connection to the network. Until the new connection is established, the node cannot utilize network services.

D NETWORK LAYER FUNCTIONS

Mobile Ad-Hoc Networks (MANET) are extensions to existing routing information protocols that accommodate volatile routing topology changes. MANETs deal with router-to-router connectivity tables that detail the path information will travel to arrive at a node. MANETs are independent of the underlying technology (layer 2

protocols) so it is quite possible that a MANET domain will include several different network segment standards. The Internet Engineering Task Force has sponsored a development group to build viable standards-based MANET protocols that will run mesh networks in the future.

Because every node in a MANET functions as a router, the network layer's involvement with mesh networking is vital for success. The specific network layer protocol must meet many requirements for MANETs. The protocol must allow nodes to discover neighboring nodes and routes through the networks, and it must allow for timely dissemination of the network map. In addition, the protocol must be dynamic and allow for nodes to enter, exit, and move through the network while providing updates to the network of these developments.

There are two types of MANET protocols, and each takes a different approach for developing mesh networks. One protocol is a proactive protocol and the other is a reactive protocol. They will be described next.

1. Proactive Protocol

The proactive protocol, as the name implies, identifies a network path prior to the user needing a route in order to send a message. The protocol will send periodic hello messages to maintain an accurate map of neighboring nodes. This information is then forwarded through the network until every node has an accurate picture of the network. When a user needs to send a message, the node simply looks at the routing tables for a route to the destination and sends the message. Network convergence in this type of protocol is front-loaded, meaning that multiple messages will be sent between nodes prior to developing a full picture of the network. Proactive protocols consume network resources while maintaining convergence even when the network is idle.

2. Reactive Protocol

This protocol takes the opposite approach from the proactive one. The reactive protocol will not discover a route until a user requests to send information. Once a user requests to send information to a specific address, the protocol will send out a route request message that will be forwarded through the network. After the destination receives the request message, it will send a route reply back to the source annotating a

path to the destination. The node will then send the information utilizing the discovered path. Once a route is discovered, the nodes can maintain the route information in their routing tables giving them partial convergence. Therefore, as time passes and network traffic increases, convergence within the network will be achieved.

3. Protocols in Use

As mentioned previously, only a few protocols can be implemented to run MANETs, and each of these function in a different manner (they will not be described here). Some of the main protocols are Optimized Link State Routing (OLSR), Ad-Hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Topology Dissemination Based on Reverse Path Forwarding (TBRPF). These protocols are currently being used to implement MANET networks.

E. MESH NETWORK CONCERNS

Mesh networks described in this chapter have many features and provide much promise and potential. There are, however, concerns and problems that must be overcome before mesh can be implemented on a large scale. These concerns will be described next.

1. Power Consumption

Power consumption in any electronic device is a concern to the engineers that design the equipment. For a mesh network that operates in a military environment, power consumption is a huge concern. One of the main goals of mesh networking is to allow nodes or stations to maneuver through the battlefield while maintaining network connectivity. Mobile nodes, in particular, require methods to allow them to maximize their power consumption since they will be powered by transportable DC power sources. There are various methods to help minimize this problem and techniques can be applied in both hardware and software design.

2. Security

Securing the network is a priority in any military network, including mesh networks. Since the network uses the RF medium, new challenges arise because RF transmission can be heard by everyone, including the enemy. As was the case with node

addressing, security falls within the scope of more than one layer in the OSI model. At the physical layer, which is layer 1, the information sent through the airwaves requires encryption to prevent enemy traffic analysis.

At the Data Link Layer, authentication of candidate nodes is also necessary. Before allowing a candidate node to enter the network, an authentication process must take place. In some protocols a network key or password is needed to obtain access to the network. In more advanced schemes like that in IEEE 802.16, X.509 public key certificates are used to authenticate a candidate node. Regardless of the method used, some form of authentication is required to vet a candidate node and prevent unauthorized nodes from entering the network to either passively listen or disrupt network function.

3. Scalability

As the number of nodes increase, the more congested the network becomes and the more difficult it is to manage. One can envision the amount of traffic that would be needed to allow candidate nodes to enter a large mesh network, the number of hello messages that would be sent in a large network, the number of control messages sent out by the controlling node, and the amount of data traffic sent from the networked nodes. At some point the network will cease to function because of too much congestion. Understanding the maximum capacity and designing the network to fit this capacity is necessary. There are various methods in which to keep the network from becoming too congested. These include using subnets or designating gateways to isolate network traffic.

In a military environment, physical units are discouraged from being in close proximity because indirect fire can be disastrous. Consequently, physical separation between units on the battlefield and distance between nodes will occur. Planners of mesh networks will need to strike a fine balance between having too many radios in the same mesh network and from having too much separation between nodes. With all this being said, detailed networking planning and design will be required.

4. Processing Constraints

Another important concern that developers of MANET protocols must focus on is the processing power needed to operate these protocols. The nodes running these

protocols will operate apart from fixed infrastructure and power sources. Therefore, these protocols must account for nomadic and mobile nodes that do not have large processors with unlimited resources and develop their protocol accordingly.

F. SUMMARY

Military communication has evolved and the requirements for new devices have increased. Military networks are actively utilizing digital information and the need to push this information further down the chain of command is growing. Mesh networking is a promising technology that is well-suited for military environments; in fact, the concept of mesh was developed for military applications. Military environments are dynamic and the technology needed to operate in this environment needs to be dynamic as well. The underlying information that controls mesh networks and enables user communications is vital to functioning mesh networks. This technology needs to control many different scenarios and be developed with the limitations of mobile nodes in mind. Mesh technology could be the technology that is able to bridge the last tactical mile.

IV. EXPERIMENT AND EQUIPMENT OVERVIEW

A. FIELD EXPERIMENT DISCUSSION

The experiments at Camp Roberts were used to test the conceptual networked communications architecture that can be used for Distributed Operations (DO) units, ultimately, for Exercise Sea Viking '08. These tests built upon the work that was done at previous Camp Roberts' experiments and the data from other students' theses. The ultimate goal is to extend the tactical internet to DO units with wireless, lightweight, user-friendly, hand-held devices that can be used to transmit and receive digital data. The architecture is based on the concept of a lower layer mesh (access) layer and a long range, battlefield backbone connection.

The mesh layer is used by the DO platoon for intra-platoon communication. The mesh network's capabilities are well-suited for the DO platoon and fill the need for a self-forming, self-healing network that can utilize many different applications for platoon communication.[6] This mesh network is then connected to the company headquarters with a longer range battlefield backbone connection. The long range connections are used to send and receive digital data between the platoon and company headquarters. Without these connections, the platoon would be isolated from the larger tactical internet.

The equipment that was used for the Camp Roberts experiments, both hardware and software, are described in this chapter. A description of the experiments, and the results from those experiments, are described in the next chapter.

B. DESCRIPTIONS OF EQUIPMENT USED

The next section will describe the equipment and software employed during the Camp Roberts experiments. The equipment described below is separated into three categories. The first category describes the equipment for platoon level and below mesh layer. The second illustrates the battlefield backbone equipment used to connect the platoon level to higher headquarters. The last category describes the software that was used in the conduct of experiments.

[6] Chapter III describes mesh networks in full detail.

Before describing the devices, an explanation of why INTER-4 products were chosen should be provided. INTER-4, a division of the Sierra Nevada Corporation based out of San Francisco, develops mesh networked devices for military applications. In the authors' opinion, the INTER-4 product line with embedded ITT mesh cards provide the most mature mesh product line on the market today. Their equipment uses COTS technology, along with Advanced Encryption Standard (AES) security, to provide a robust and easy-to-use mesh network that can be utilized to transmit and receive data.[7] Their equipment also meets military packaging standards for environmental conditions and vibration. Finally, INTER-4's equipment has been used extensively in combat environments by the U.S. Army, and the company is constantly soliciting feedback from the end-users to improve their product.[8]

1. Mesh Wireless (Access) Devices

a. INTER-4 Tacticomp 1.5

According to the INTER-4 website, "The INTER-4 Tacticomp is a Wireless and GPS enabled military hand-held computer designed for field use. The Tacticomp offers a unique level of integration in a small, lightweight and rugged design." [6] The Tacticomp was used at the platoon level to create mesh networks in the Camp Roberts' field experiments. The Tacticomp was used to demonstrate that meshed nodes have the ability to transmit and receive voice over Internet Protocol (VOIP), streaming video, position location information, and chat messages. The Tacticomp runs the Windows CE operating system along with General Dynamics' Soldier Tactical Software (STS) which is described in more detail below. The Tacticomp utilizes a 400 MHz Intel XScale Processor. In addition, the Tacticomp contains ITT's Mesh Enabled Architecture (MEA) mesh cards for use as a radio interface to transmit and receive information (the MEA cards are described in further detail below). The communication range of the Tacticomp is approximately 1 kilometer line of sight (LOS) while operating in an omni-directional mode. Figure 8 shows INTER-4's Tacticomp 1.5.

[7] AES encryption occurs at layer 3 in the INTER-4 product line.

[8] The employment of the INTER-4 equipment has only been used in small scale deployments and, to date, the network information has not been bridged into the SIPRNET.

Figure 8. Tacticomp 1.5

b. INTER-4 T-6

The INTER-4 Tacticomp 6 (T-6) is a larger version of the Tacticomp 1.5 and contains many of the same features (the T-6 runs the same STS software as the Tacticomp). This device utilizes a Windows XP Professional operating system with an Intel 1.8 GHz Pentium M processor. The T-6 can operate in a wireless mode (it also contains the ITT MEA mesh card) or on a local area network (LAN). In the Camp Roberts experiments, the T-6 was employed in the Light Reconnaissance Vehicle (LRV), and in the Tactical Operations Center (TOC), which simulated the role of a higher-level headquarters. The wireless interface was disabled and the T-6 communicated with other devices solely through the TOC LAN. The T-6 is displayed in Figure 9.

Figure 9. Tacticomp T-6

c. INTER-4 T-5

The T-5, the latest hand-held product from INTER-4, provides much of the same capability as the T-6 in a smaller and lighter form factor. This device incorporates an Intel 1.0 Ghz Pentium M processor running Windows XP Professional. The T-5 provides a much improved daylight-readable screen capable of displaying full color and detail even when viewed in direct sunlight. The T-5, pictured in Figure 10, utilizes the same ITT mesh card technology as the other INTER-4 products.

Figure 10. Tacticomp T-5

d. INTER-4 MMR (Micro Mesh Router)

According to the INTER-4 website, "The INTER-4 Omni-directional Micro Mesh Routers (MMR) is a wireless device that transmits data up to 12 miles." [7] The MMR functions as part of the network to extend the range of the mesh network, and allows two or more separated meshed units to communicate with another. Although the device is labeled as a router, the device simply serves as a bridge between geographically separated mesh networks; it does not perform layer 3 routing. The MMR was used to extend the range of meshed nodes during the Camp Roberts experiments; the MMR extends the range by acting as a bridge between mesh networks. Additional MMR offerings include a five watt amplified variant, as well as a model that supports enhanced directional capability. Figure 11 depicts an MMR.

Figure 11. INTER-4 MMR

e. ITT MEA Mesh Card

The ITT MEA card—also manufactured by Motorola as the WMC 6300—is a Personal Computer Memory Card International Association (PCMCIA) radio device used by hand-held computers to enable mesh network communication. A key point for this device is that this is not an 802.11 PCMCIA device. The firmware inside the cards allows for self-forming and self-healing networks to be developed with very little user input. There are two variants: a 2.4 GHz for public use, and a frequency shifted 2.X GHz card for Department of Defense use. The variant used in the Camp Roberts experiments were the frequency shifted cards. ITT claims that the maximum shared data rate is 2 Mbps with a burst rate capability of 6 Mbps. ITT also claims that the cards can transmit up to one mile LOS. These devices use the Quadrature Division Multiple Access (QDMA) modulation scheme where three channels are dedicated to transmit data and one channel is for network control. This modulation scheme was designed, and is well-suited for, ad-hoc or mesh environments. Although these cards work with the internet protocol, frame forwarding between nodes is performed at the Data Link layer. These cards are incapable of multicast or acting as a layer 3 router. Figure 12 shows the ITT mesh card.

Figure 12. ITT Mesh PCMCIA Card

f. Virtual Access Point (VAP)

The VAP is a layer 2 bridging device, similar to an traditional IEEE 802.11 access point, that contains a wireless MEA radio interface and two Ethernet interfaces. It is used to bridge the wireless mesh and Ethernet network segments. For the Camp Roberts experiments, the VAP was connected to the same LAN as the T-6. When the T-6 sent or received information from the Tacticomp 1.5 mesh devices, the information would be funneled through the VAP and bridged onto the appropriate network. This device provides flexibility for operators and allows communication from a mesh network to be transferred into a wired LAN. The VAP's dimensions are 10"x 8"x7", and can be easily moved or transported. Figure 13 depicts a VAP.

Figure 13. INTER-4 VAP

2. Battlefield Backbone Device

a. Redline AN-50e

According to Redline's product website, the AN-50e is "…Redline's high speed wireless Ethernet bridge configured for point-to-point (Ptp) operation, with point to multipoint (PtMpt) operation capabilities. Accommodating both backhaul and access functions…"[8] The AN-50e firmware is based upon the IEEE 802.16-2001 standard.

For the Camp Roberts experiments, this device was used in a battlefield backbone capacity and bridged the mesh (access) layer devices (described above) to a simulated higher level command post. This link connected the Tacticomp 1.5s with the T-6 operating on the TOC LAN. In trying to develop a tactical internet solution for DO, this is an extremely important communication link because lower level mesh units likely will not be in RF range of higher level command posts. Redline claims that the AN-50e is capable of 72Mbps of total throughput and can extend to a range of 30 miles or more depending on antenna type. High gain, directional antennas will increase the range of the radios. The system operates in the 5.470-5.725 GHz and 5.725-5.850 GHz bands. Figure 14 displays the Redline AN-50e.

Figure 14. Redline AN-50e

b. Redline AN-80i

Another Redline radio used for long range battlefield backbone connections is the AN-80i (beta version). This radio was also used in the Camp Roberts experiments to connect the Tacticomp 1.5s with the T-6 operating on the TOC LAN through the LRV. This radio is similar to the AN-50e but has a reduced form factor, greater throughput, and greater range than the AN-50e.

3. Software

a. IX-Chariot

IX-Chariot is a performance emulation software tool that can be used to assess network performance. This software was used to perform throughput tests between various nodes in the Camp Roberts experiments. In order to use the tool, the console program must be loaded on a computer attached to the LAN. The console program is used to manage the throughput tests. Endpoint software must be loaded onto

the devices that participate in the throughput test experiments. For a test to occur, the IP addresses of the endpoint nodes must be typed into the console program. The console program then distributes a script to the endpoints and the test will commence. The console program collects the information from the nodes and provides information and graphs to judge network efficiency. This software was used to test data throughput between nodes in the mesh network and between the battlefield backbone links.

b. STS Software

STS Software was developed by General Dynamics for the British BOWMAN program and is used within INTER-4's product line. There are three main software programs that can be used to communicate within the mesh network. The programs are: STS voice, which is a VOIP application used for voice communication; STS chat, which is used to send/receive chat messages from any node in the mesh network; and STS C2, which is a command and control program that displays position location updates graphically on military maps. The STS software is also compatible with Force Battle Control, Brigade and Below (FBCB2), which will replace Command and Control Personal Computer (C2PC) for the Regiment level and below for Marine units in the near future. This software was used in the Camp Roberts experiments to demonstrate the ability to communicate using multiple applications across a mesh network. Figure 15 shows a screen shot from the STS C2 program.

Figure 15. STS SA Program

4. Equipment Tested in the Lab but not Employed at Camp Roberts

a. Dismounted-Digital Automated Communications Terminal (D-DACT), MMC Computer Company Modular Personal Computer (PC)

D-DACTS and MMC Micro Tablet PC's are Personal Digital Assistants (PDA) that were initially evaluated in a lab environment. They were used to test the compatibility with the ITT MEA card. The cards were placed in the PCMCIA slots of each device, and these devices were used to check connectivity across the mesh network. The initial results were positive as ping tests were sent across the connection between the devices. However, the D-DACTS in particular, were not capable of maintaining their mesh connections for an extended period of time. The authors speculate that the MEA drivers were not compatible with the operating system running on the D-DACTs.[9] Because of these problems, the D-DACTS were not used in the Camp Roberts experiments. Furthermore, the devices did not utilize the appropriate software encryption program to enable communication with the INTER-4 devices.[10] Further tests should be performed on various PDA's with MEA cards inserted. Figure 16 depicts a D-DACT and a Modular PC.

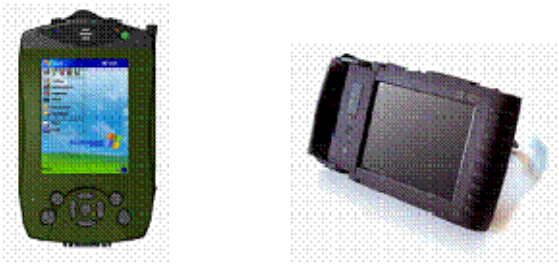

Figure 16. These photos depict a D-DACT and a Modular PC, respectively.

C. SUMMARY

This chapter described the purpose of the Camp Roberts experiments and the equipment used to conduct them. The equipment was broken down into three categories: equipment for platoon level mesh (access), equipment for battlefield backbone

[9] The D-DACT runs Windows Pocket PC 2002 as its operating system.

[10] The INTER-4 product line uses a proprietary software-implemented AES encryption program. Non-INTER-4 devices are not compatible without this software load.

connections, and the software used to test functionality of the simulated DO tactical internet. The next chapter will describe the experiments at Camp Roberts that were designed to simulate a DO network and detail the results.

V. FIELD EXPERIMENTATION

The field experimentation conducted in support of this thesis occurred during Naval Postgraduate School's Tactical Network Topology (TNT) experiments held in May and August 2006 at Camp Roberts Army National Guard Base north of Paso Robles, CA. This chapter outlines each TNT experiment in detail by providing a scenario overview, a graphical representation of the architecture and equipment employed, and the results of each test conducted during the evolution.

A. TACTICAL NETWORK TOPOLOGY FIELD EXPERIMENT 06-3 (JUNE 2006)

1. Background

TNT 06-3 served as a starting point in conducting the research required to support this thesis. These initial experiments focused on integrating a wireless mesh network with an IEEE 802.16 link in a lab environment. This test period also laid the foundation for planning and coordinating the follow-on experimentation conducted at Camp Roberts during the next TNT experiment in August 2006.

2. Network Architecture

The network architecture created for this experiment centered on the Redline Communications AN-50e radios and the IEEE 802.16 link that was established between two of these units. One AN-50e radio was programmed as the base station and the other AN-50 was programmed as a subscriber station. The IP addresses for the master and slave stations were 192.168.25.4 and 192.168.25.2, respectively.

Next, the mesh network was created by using two INTER-4 Tacticomp 1.5's and a Versatile Access Point (VAP). INTER-4 incorporated the ITT 2.x PCMCIA wireless mesh card across their product line and developed a proprietary 256-bit Advance Encryption Standard (AES)[11] software encryption algorithm and added it to the system

[11] AES was approved in 2003 by the National Security Administration (NSA) as a Type I encryption, suitable for use in the encryption of secret and top secret information. See CNSS June 2003 Policy No. 15, Fact Sheet No. 1 at http://csrc.nist.gov/cryptval/CNSS15FS.pdf for more details. (September 2006)

firmware.[12] The mesh cards operate in layer two of the Open System Interconnection (OSI) Reference Model, and implements the wireless mesh connectivity through the ad-hoc, self-healing, and self-forming functionality designed into the network card. The basic architecture described in this lab experiment is shown in Figure 17 below.

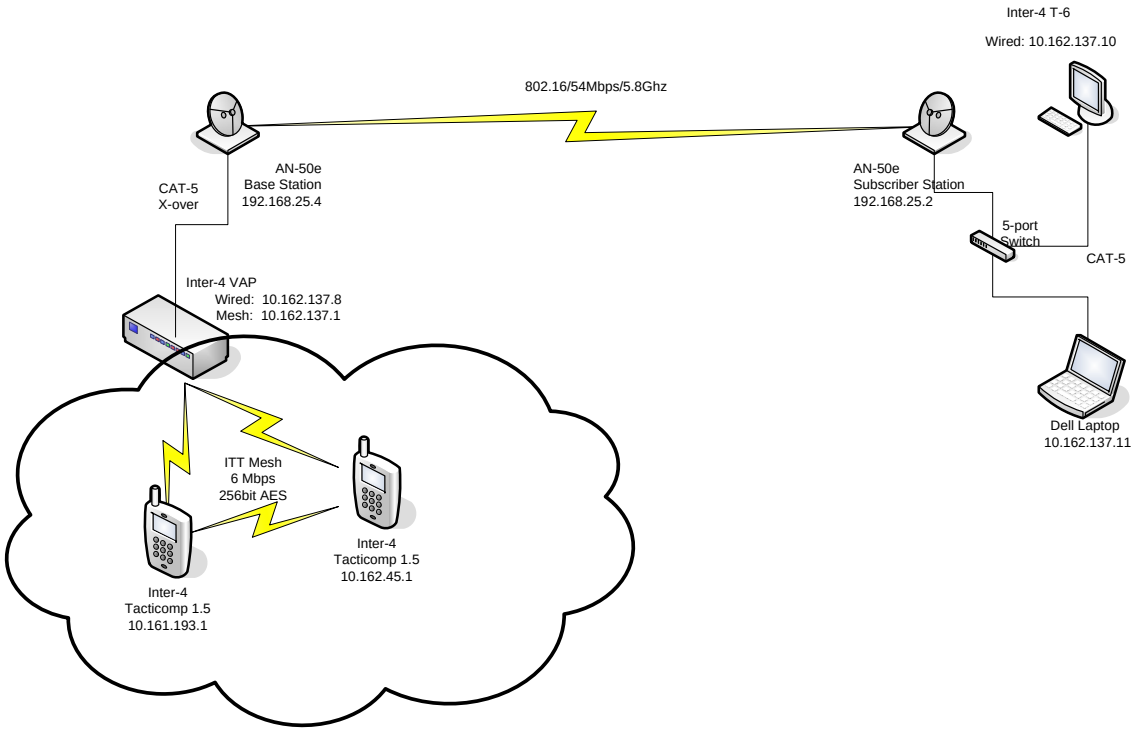

Figure 17. Mesh Network and 802.16 Lab Experiment

3. Test Results

After establishing the mesh network connectivity, attempts were made to bridge the wireless mesh network cloud with the 802.16 link. The VAP was designed for this specific function, and upon proper configuration the T-1.5 handhelds could send ping packets across the wireless mesh network through the VAP acting as a bridge and across the 802.16 link to the laptop connected to the distant end 801.16 subscriber station. The ping functionality also worked in the opposite direction, and we concluded our initial lab experiments having achieved a baseline from which to conduct further experimentation.

[12] Even though NSA approved AES as Type I cryptography, the specific implementation of this algorithm in the Tacticomp product line has not been reviewed and certified by NSA. The U.S. Army, however, has been granted an interim waiver to operate these devices.

4. TNT Field Experiment 06-3 Summary

The results of this lab experiment were critical in providing the necessary details for conducting additional testing. This basic test set-up formed the foundation for planning and coordinating the next round of follow-on experimentation and provided clear guidelines for future equipment configuration and operation for both the INTER-4 products and the Redline radios.

B. TACTICAL NETWORK TOPOLOGY FIELD EXPERIMENTATION 06-4 (AUG 2006)

1. Background

The next round of experiments also took place at Camp Roberts, CA, during the subsequent TNT field experiments scheduled in the month of August 2006. Due to the varied terrain and limited line of site (LOS) opportunities, this central California National Guard base provided an ideal location for conducting these tests. The experiments conducted during this evolution served as the principle means of testing and data capture in support of this research, with the scope of the experimentation divided into two main scenarios: (1) mesh only and (2) mesh-802.16 long-haul bridge integration. The testing during both scenarios focused on capturing qualitative data related to capabilities involving VOIP, instant chat, streaming video, and situational awareness (SA) or position location information (PLI) applications or functionality. These capabilities remain critical to the effective command and control of Distributed Operations units and their leaders.

The first scenario consisted of layer two mesh devices only and was designed to simulate three squads operating independently within an area spanning several square kilometers while maintaining network connectivity with each other over a wireless mesh network, also known as the access layer. The second scenario added to the first by incorporating an 802.16 broadband link, also referred to as the battlefield backbone, to the meshed network.[13] The link provides the critical network connectivity back to a Tactical Operations Center (TOC) or Combat Operations Center (COC) likely located tens of kilometers away from the operating squads.

[13] IEEE 802.16 provides a standards-based technological solution for the battlefield backbone space between the higher echelon commands supported by systems found in Table 1 and the company and below headquarters. In this scenario, we bridge two parts of a DO platoon separated by distance.

2. Scenario One Network Architecture

A graphical representation of the network architecture deployed during scenario one is provided below:

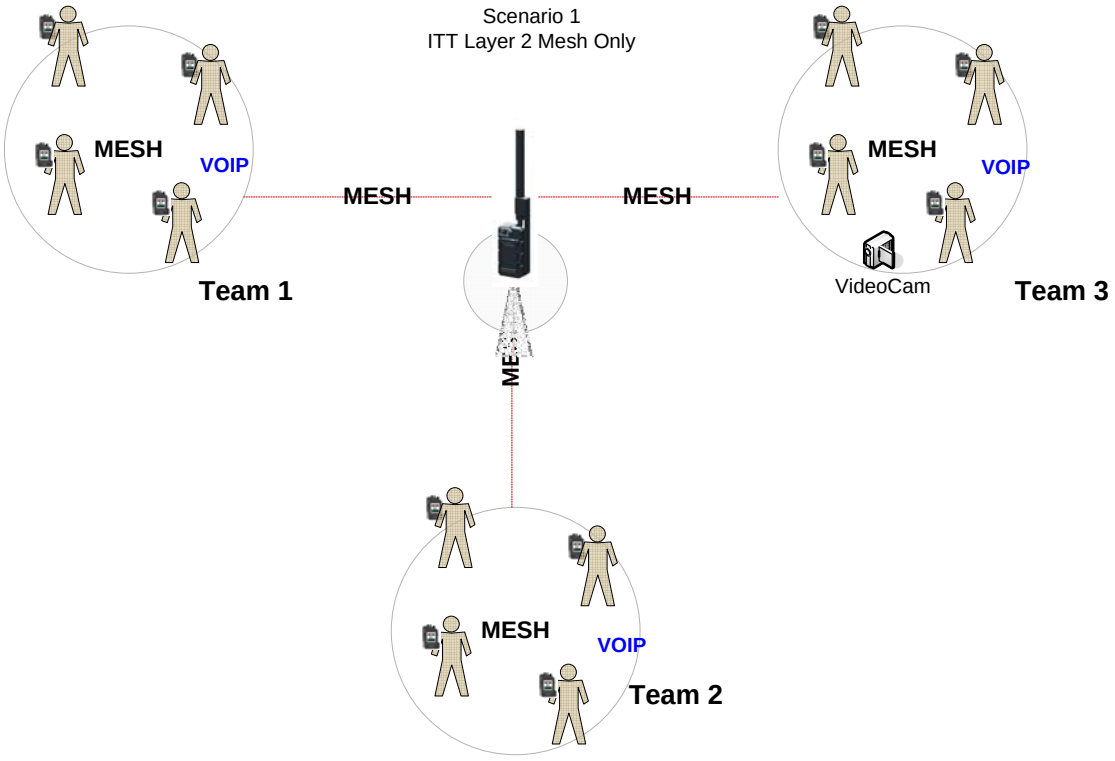

Figure 18. Scenario One Wireless Mesh Network Diagram

The mesh network utilized an INTER-4 Omni-directional Micro Mesh Router (MMR) that acted as a network bridging device, further extending the capable range between each squad. Similar to the Tacticomp ruggedized handheld computers, the MMR also features an ITT 2.x PCMCIA Enhanced Wireless Router (EWR) card that enables this device to send and receive the mesh transmissions and utilizes a higher layer-2 routing weight. In essence, the cared employs an algorithm such that if a node already has an alternative route to it s destination, then it will not use the MMR. In other words, "if you have a choice, don't route through me." The INTER-4 handheld computers, the

MMR, and the VAP were configured with the Media Access Control (MAC) addresses and Internet Protocol (IP) addresses provided in Table 2 below:

Device Name	IP Address	MAC
T-6/TOC	10.137.227.1	00-05-12-0A-89-E3
LAPTOP/TOC	10.143.79.1	00-05-12-0A-8F-4F
T-1.5/1stSquad	10.137.63.1	00-05-12-0A-89-3F
T-1.5/1stSquadAlpha	10.158.56.1	00-05-12-0A-9E-38
T-1.5/2ndSquad	10.157.222.1	00-05-12-0A-9D-DE
T-1.5/3rdSquad	10.135.76.1	00-05-12-0A-87-4C
T-1.5/3rdSquadAlpha	10.158.118.1	00-05-12-0A-9E-76
MMR	10.136.174.1	00-05-12-0A-88-AE

Table 2. Scenario One Network Addressing

Initial set-up proved to be a simple and straightforward process. All INTER-4 Tacticomp products are configured with a static MAC and IP configuration settings for their ITT wireless mesh cards. This "hard-wired" configuration minimizes operator set-up procedures, eliminates end-user input error, while allowing the self-forming, self-healing, ad-hoc capabilities to establish timely and reliable access layer network connectivity.

3. Test Results

Table 3 describes each event planned during the first scenario. A majority of these tasks were successfully completed, and those that were not accomplished could have been completed if more time was allotted and/or configuration issues were resolved between the VAP and the network throughput analysis program, IX Chariot.

Event	Short-title	Experiment Description	Status
INTER-4 MESH VOIP			
1-1	TOC TO SQD 1	Demonstrate VOIP call from the TOC to Sqd 1.	Accomplished
1-2	TOC TO SQD 2	Demonstrate VOIP call from the TOC to Sqd 2.	Accomplished
1-3	TOC TO SQD 3	Demonstrate VOIP call from the TOC to Sqd 3.	Accomplished
1-4	SQD 1 TO SQD 2	Demonstrate VOIP call from Sqd 1 to Sqd 2.	Accomplished
1-5	SQD 1 TO SQD 3	Demonstrate VOIP call from Sqd 1 to Sqd 3.	Accomplished
1-6	SQD 2 TO SQD 3	Demonstrate VOIP call from Sqd 2 to Sqd 3.	Accomplished
INTER-4 MESH Video			
2-1	SQD 3 TO TOC	Transmit video from Sqd 1 to TOC	Accomplished
2-2	SQD 3 TO SQD 1	Transmit video from Sqd 1 to TOC	Accomplished
INTER-4 MESH Chat			
3-1	SQD 1 send message	Demonstrate chat capability with Sqd 1 transmitting to all nodes.	Accomplished
3-2	SQD 2 send message	Demonstrate chat capability with Sqd 2 transmitting to all nodes.	Accomplished
3-3	SQD 3 send message	Demonstrate chat capability with Sqd 3 transmitting to all nodes.	Accomplished
3-4	TOC send message	Demonstrate chat capability with TOC transmitting to all nodes.	Accomplished
INTER-4 MESH PLI			
4-1	PLI test	TOC, Sqd 1, Sqd 2, Sqd 3 will affirm that PLI information is visible and accurate.	Accomplished
INTER-4 MESH IX-Chariot			
5-1	SQD 1 TO TOC	Conduct throughput test from Sqd 1 to TOC.	Accomplished
5-2	SQD 2 TO TOC	Conduct throughput test from Sqd 2 to TOC.	Not Accomplished
5-3	SQD 3 TO TOC	Conduct throughput test from Sqd 3 to TOC.	Not Accomplished
5-4	SQD 1 TO SQD 2 TO TOC	Conduct throughput test from Sqd 3 thru Sqd 2 back to the TOC.	Accomplished
INTER-4 MESH Range Test			
6-1	SQD 3 VOIP to TOC	Sqd 3 will move to the edge of RF coverage and then transmit VOIP to the TOC.	Not Accomplished
6-2	SQD 3 VIDEO to TOC	Sqd 3 will move to the edge of RF coverage and then transmit Video to the TOC.	Not Accomplished
6-3	SQD 3 PLI	Sqd 3 will move to the edge of RF coverage; Sqds 1, 2 and TOC will affirm PLI information.	Not Accomplished
6-4	SQD 3 CHAT MESSAGE	Sqd 3 will move to the edge of RF coverage and then transmit chat message to all nodes. Sqd 1, 2 and TOC will affirm receipt.	Not Accomplished

Table 3. Scenario One Test Objectives

Figure 19 provides aerial imagery with a graphical overlay depicting the DO scheme of maneuver and network connectivity. The Soldier Tactical System (STS) Software provides this imagery while integrating unit situational awareness (SA) mapping functionality.

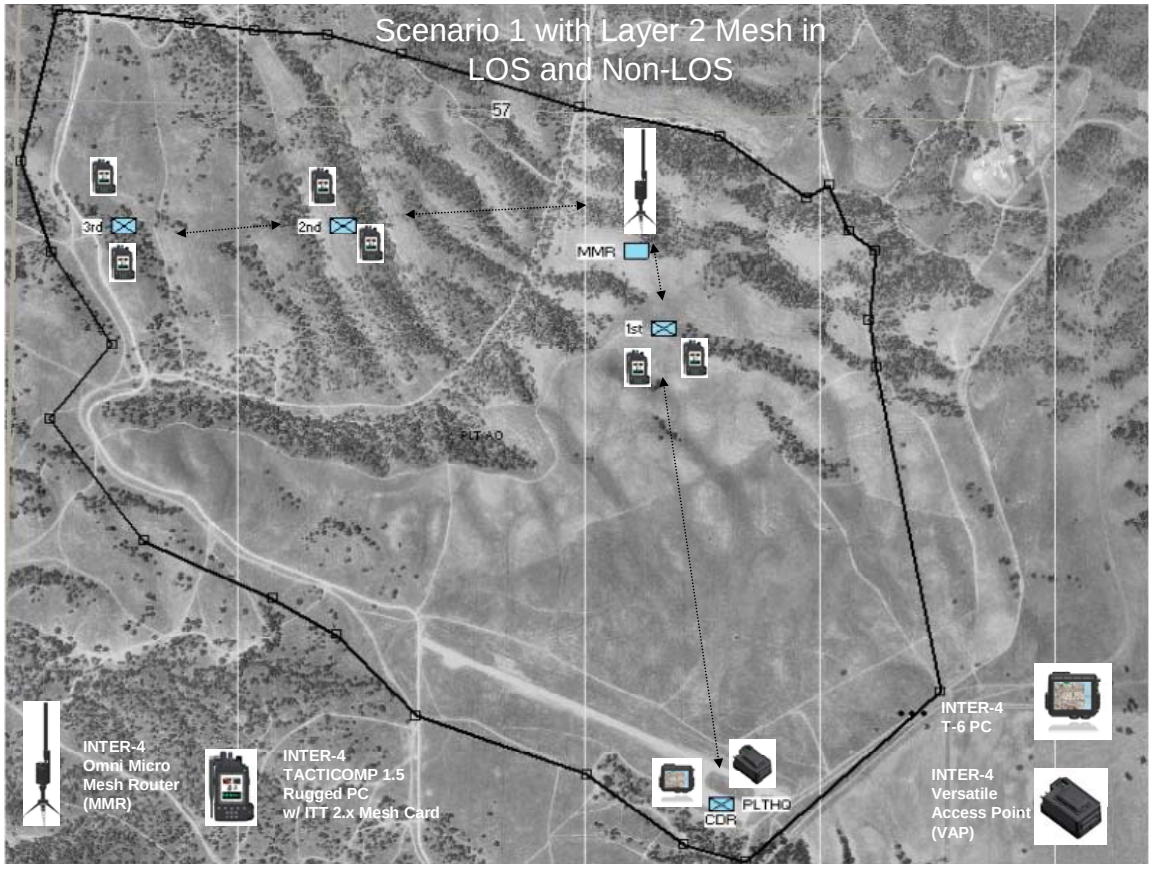

Figure 19. Scenario One Access Layer Experiment

The Tacticomp PCs also incorporate a mesh network management tool that enables each device operator to view real-time status of the wireless meshed network. This program, called Mesh View, provides each networked user with specific information relating to connected nodes up to one hop away. Figure 20 provides an example of the Mesh View application captured during the early stages of scenario one.

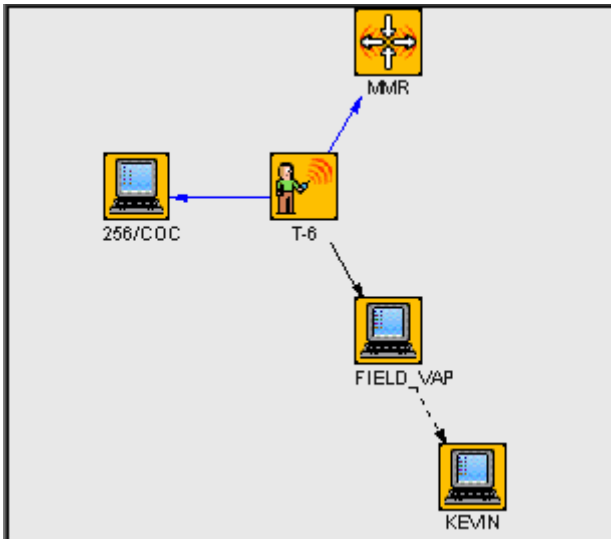

Figure 20. Net Monitoring

In order to conduct the streaming video portion during scenario one, a Tactisight compact helmet-mounted video camera was added as a component to a Tacticomp 1.5 located in Squad 3. The video feed, captured at a rate of 5 frames per second, was successfully transmitted through the mesh network and viewed at the TOC in real time, as depicted in Figure 21.

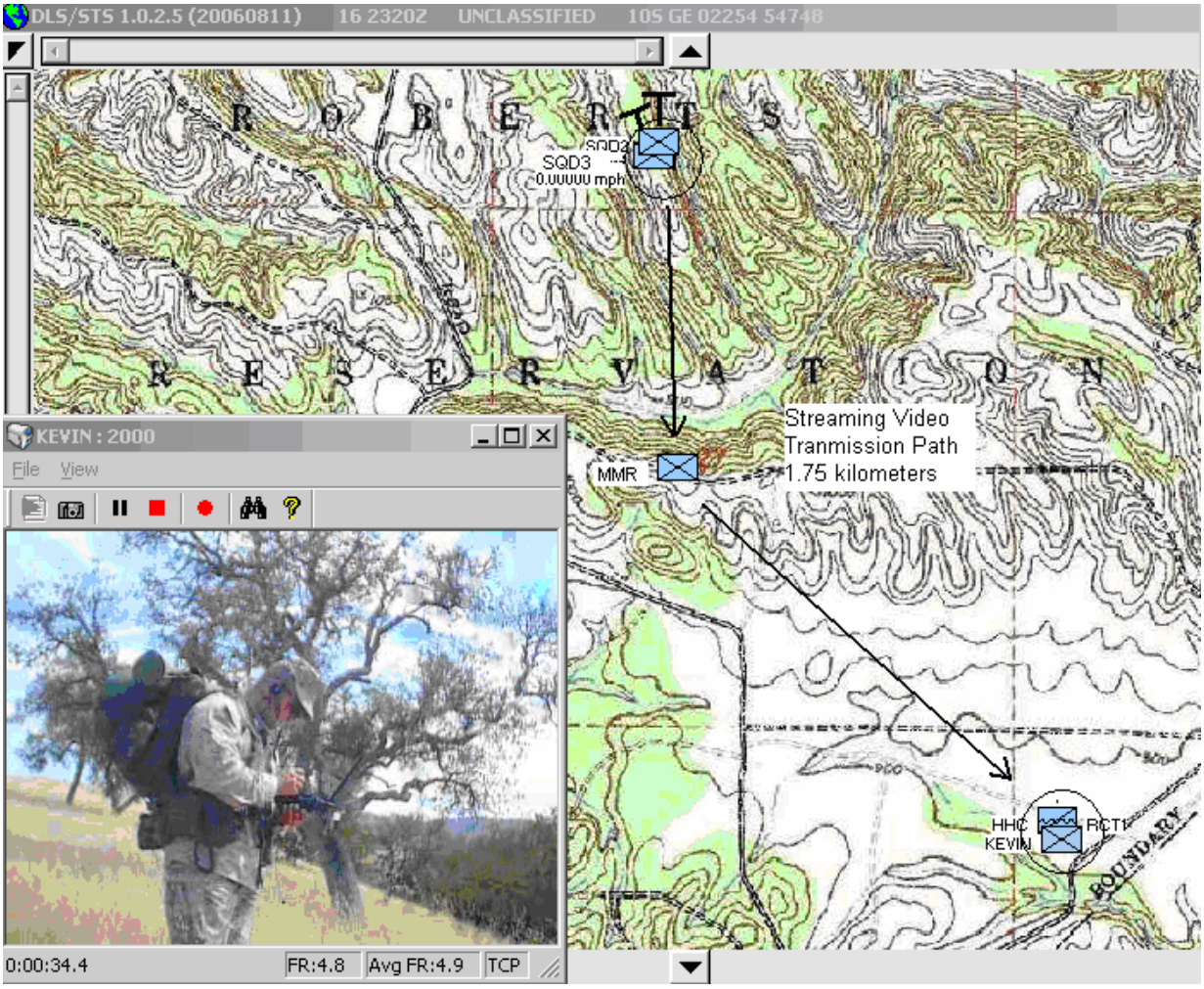

Figure 21. Streaming Real-Time Video

The ability to send and receive text chat in both a discrete mode (individual node to node) and in a broadcast mode,[14] similar to a conventional chat room application, was successful. Figure 22 depicts a sampling of text chat traffic.

[14] The Soldier Tactical Software application utilizes unicast transmissions to support the broadcast mode of text chat operation.

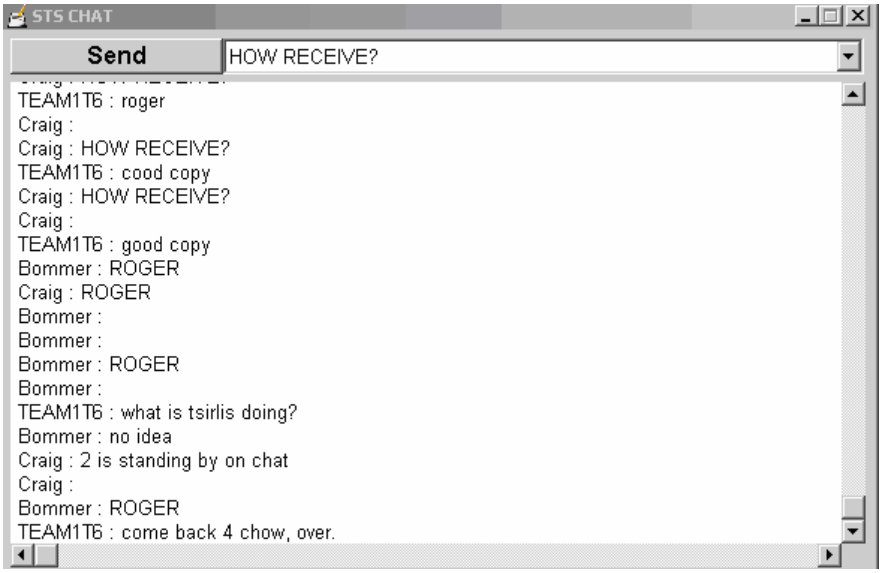

Figure 22. Text Chat

Throughout scenario one, all nodes successfully maintained situational awareness with each other through the timely automated dissemination of PLI data across the network. The STS software displays this PLI data over digital imagery for scales ranging from 1:10K or larger and over topographical maps for scales smaller than 1:10K. Figure 23 represents a large scale SA display while Figure 24 represents a smaller scale SA view. Only the PLI data is transmitted when updating node locations, all digital imagery and mapping utilities reside on Tacticomp hard-drives.

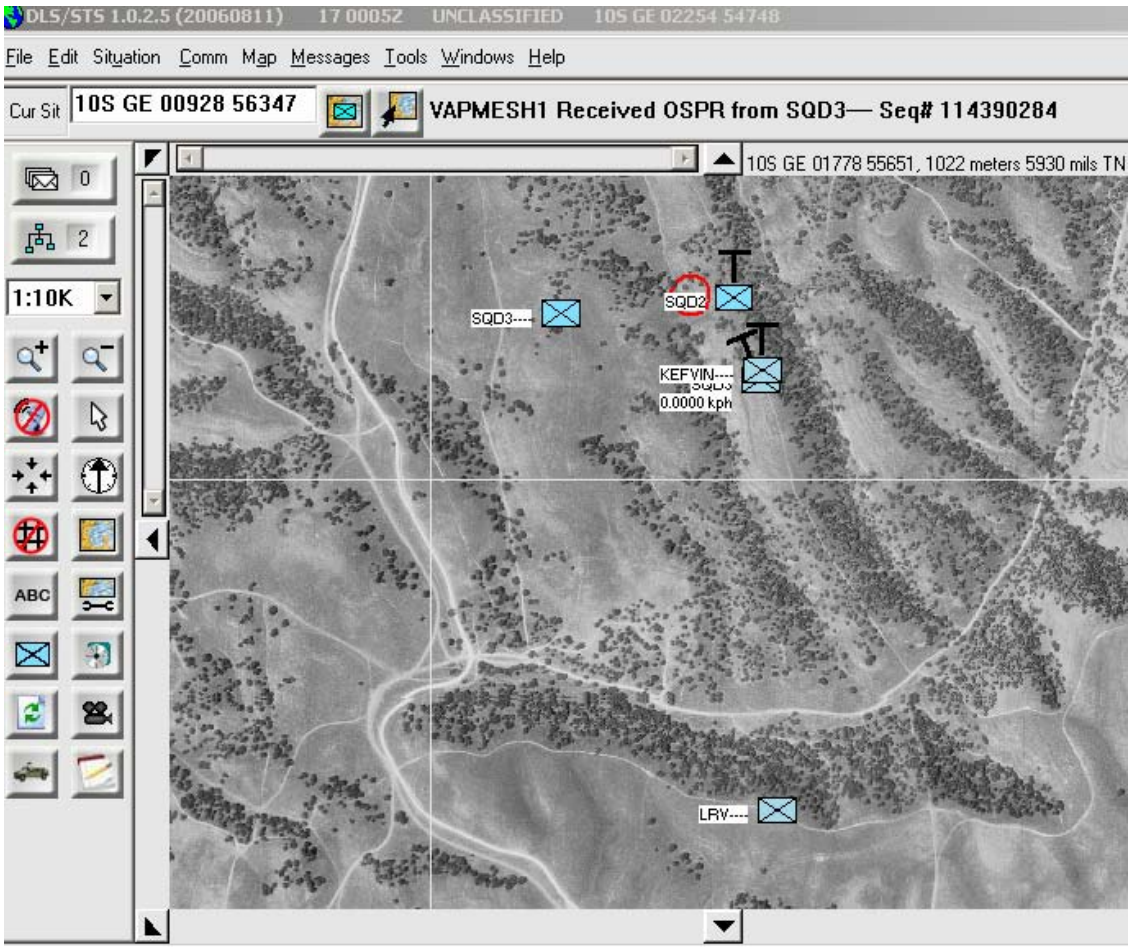

Figure 23. Large Scale (1:10K) SA Display

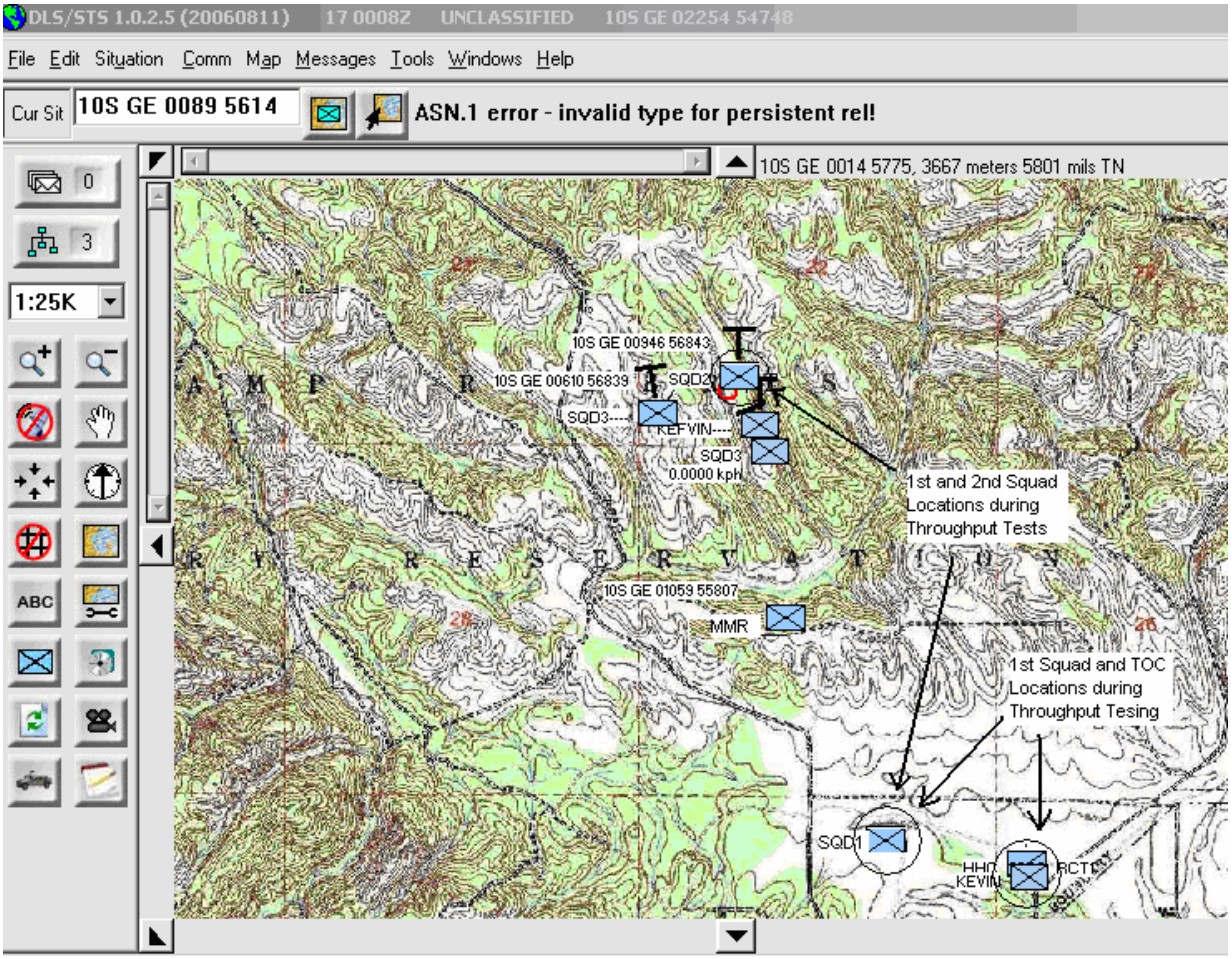

Figure 24. Small Scale (1:25K) SA Display

Throughput testing was conducted utilizing IXChariot network performance analysis software. The IXChariot's console program was loaded on a Panasonic CF-48 Toughbook that was temporarily connected to the mesh architecture via an Ethernet switch connected to the VAP, and all Tacticomp 1.5 PCs were loaded with the IXChariot client software. Several throughput tests were captured from the Toughbook representing wireless transmissions between squads and between the TOC and selected squads. Figures 25 and 26 highlight two different throughput performance results, with the first displaying the results captured between squads 1 and 2, and the second displaying the results of throughput capacity recorded between squad 1 and the TOC. Between these two tests, throughput across the mesh network averaged 650 kbps.

Figure 25. IXChariot Throughput Results between Squads 1 and 2

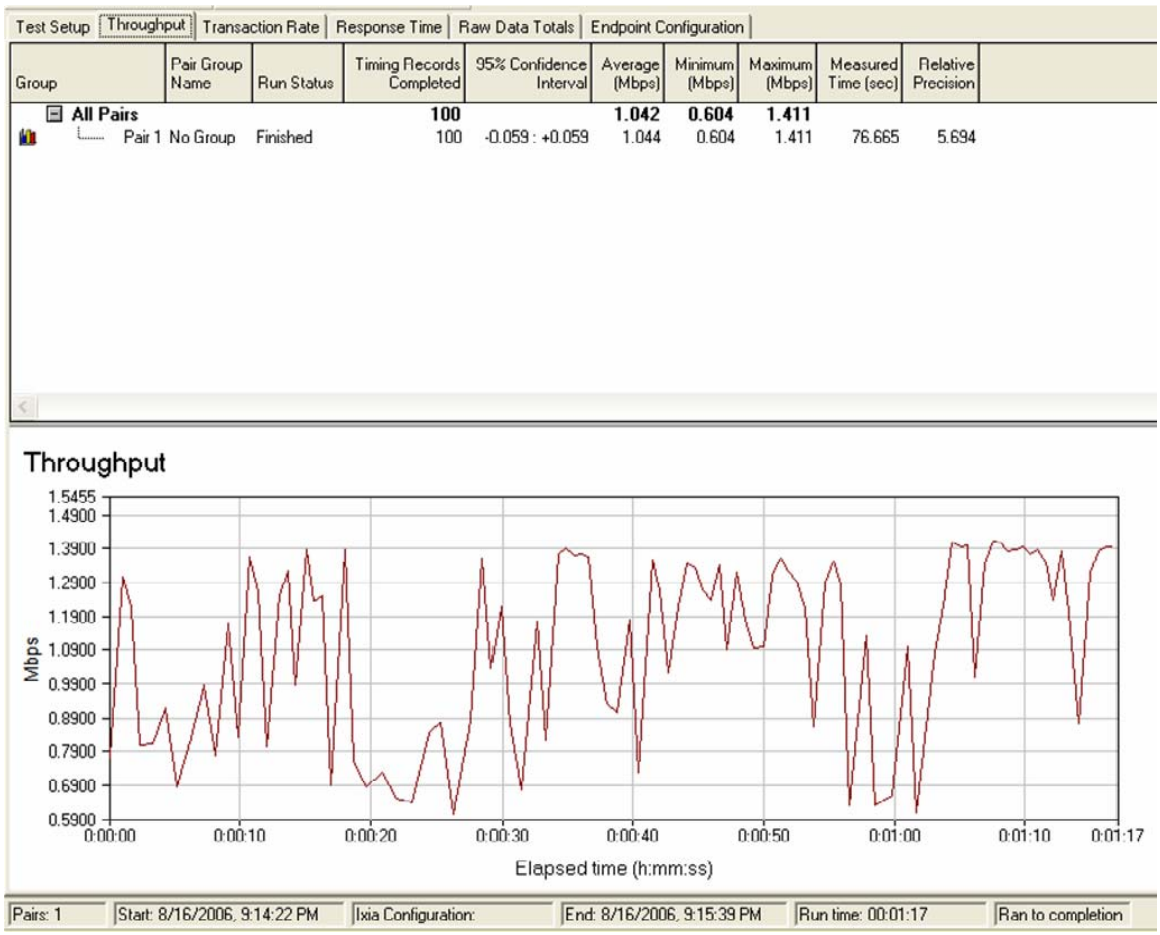

Figure 26. IXChariot Throughput Results between TOC and Squad 1

4. Scenario Two Network Architecture

The second experiment evaluated the integration of an 802.16 long-haul capability into the tactical mesh established in scenario one. This represents the next logical level of tactical C2 architecture to the experiment. The three squads were positioned several kilometers north of the TOC while a Redline 802.16 broadband link provided the battlefield backbone, or terrestrial long-haul communications link, back to the TOC. During this next experiment, all Tacticomp devices located inside the TOC were supported by a LAN and did not utilize their wireless mesh cards. A Redline AN-50e 802.16 base station located at the TOC established a link with another Redline subscriber station installed in the Light Reconnaissance Vehicle (LRV)[15] located

[15] The LRV is a vehicular platform attempting to satisfy the desire for mobile broadband communications throughout the battlefield. This platform is based on a 2005 Toyota Tacoma 4x4 and maintains numerous wireless communications to include 802.16, 802.11, and mesh enabled technologies.

approximately 2 kilometers the northwest of the TOC. The LRV was outfitted with a VAP and a T-6, with the VAP acting as the bridge between the 802.16 battlefield backhaul and the meshed access layer. Figure 27 depicts the network implemented for scenario two.

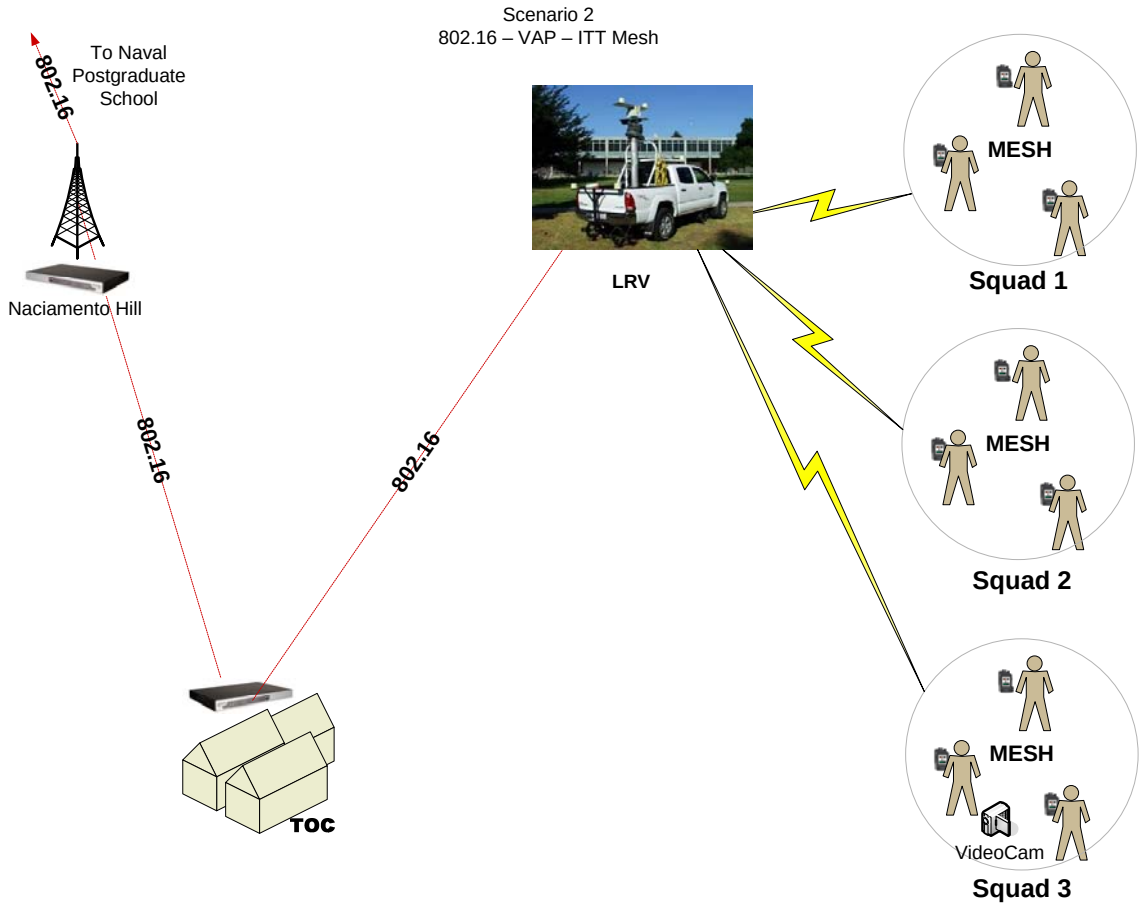

Figure 27. Scenario Two 802.16 Backhaul to Mesh Access Layer Integration

The IP address scheme from scenario one was expanded to include the Redline 802.16 radios and the additional INTER-4 Tacticomp 1.5s, T-6s, and INTER-4s latest product, a new T-5. The following table shows the addressing implemented during scenario two.

Device Name	IP Address	MAC
T-6/TOC	10.137.227.1	00-05-12-0A-89-E3
LAPTOP/TOC	10.143.79.1	00-05-12-0A-8F-4F
T-1.5/1stSquad	10.137.63.1	00-05-12-0A-89-3F
T-1.5/1stSquadAlpha	10.158.56.1	00-05-12-0A-9E-38
T-1.5/1stSquadBravo	10.128.120.1	00-05-12-0A-80-78
T-1.5/2ndSquad	10.157.222.1	00-05-12-0A-9D-DE
T-1.5/2ndSquadAlpha	10.158.229.1	00-05-12-0A-9E-E5
T-1.5/2ndSquadBravo	10.137.190.1	00-05-12-0A-89-BE
T-5/3rdSquad	10.129.135.1	00-05-12-0A-81.87
T-1.5/3rdSquadAlpha	10.158.118.1	00-05-12-0A-9E-76
T-1.5/3rdSquadBravo	10.135.76.1	00-05-12-0A-87-4C
MMR	10.136.174.1	00-05-12-0A-88-AE
T-6/LRV	192.168.99.65	00-05-12-0A-A6-50
VAP/LRV	10.135.144.1	00-05-12-0A-87-90
Redline AN-50e/LRV	192.168.99.33	
Redline AN-80i/TOC	192.168.99.26	

Table 4. Scenario Two Network Addressing

These experiments augment previous research completed by Captains Caceres and Swearingin in their thesis titled “An Analysis of IEEE 802.11b and 802.16 Technologies as Part of the Tactical Internet”, and Captains Guice and Munoz in their thesis titled “IEEE 802.16 Commercial Off The Shelf (COTS) Technologies as a Compliment to Ship to Objective Maneuver (STOM) Communications.” In both theses, the authors researched the applicability of 802.16 broadband applications in support of specific operations (Tactical Internet and STOM) and concluded that this technology remains a valid option to further the Defense Department’s focus on evolving the current battlefield into one that possesses greater network centric properties. Where Caceres and Swearingin concentrated on integrating SECNET-11 and OLSR Layer-3 mesh technology with Redline AN-50e radios, this testing focused on integrating a 256-bit AES Layer-2 mesh architecture with both Redline AN-50e and AN-80i radio platforms.

5. Test Results

Table 5 identifies the events attempted during this evolution with a focus on capturing specific levels of performance and levels of effectiveness. Events marked as

"Not Accomplished" were the result of software configuration issues between the VAP and the IXChariot program that prevented a comprehensive throughput evaluation between nodes and the TOC.

Event	Short-title	Experiment Description	Status
INTER-4 MESH/802.16 VOIP			
7-1	SQD 2 TO TOC	Sqd 1 will transmit VOIP traffic from mesh through 802.16 bridge to TOC.	Accomplished
INTER-4 MESH/802.16 Video			
8-1	SQD 2 TO TOC	Sqd 1 will transmit Video traffic from mesh through 802.16 bridge to TOC.	Accomplished
9-2	LRV TO TOC, LRV TO TOC	Sqd 3 and LRV VAP will transmit Video traffic simultaneously from mesh through 802.16 bridge to TOC.	Accomplished
INTER-4 MESH/802.16 PLI			
10-1	LRV TO TOC	TOC, Sqd 1 members will affirm that PLI information is visible and accurate.	Accomplished
INTER-4 MESH/802.16 IX Chariot			
11-1	LRV TO TOC	Throughput test using IX-Chariot from LRV T-6 to TOC.	Accomplished
11-2	SQD 2 TO TOC	Throughput test using IX-Chariot from Sqd 1 through 802.16 bridge to TOC.	Not Accomplished
11-3	SQD 1 to TOC	Throughput test using IX-Chariot from TOC to Sqd 1	Not Accomplished
11-4	SQD 2 to TOC	Throughput test using IX-Chariot from TOC to Sqd 2	Not Accomplished
11-5	SQD 3 to TOC	Throughput test using IX-Chariot from TOC to Sqd 3	Not Accomplished

Table 5. Scenario Two Test Objectives

Figure 28 provides aerial imagery with a graphical overlay depicting the DO scheme of maneuver and network connectivity implemented in support of scenario two. As with scenario one, The Soldier Tactical System (STS) Software provides this imagery while integrating unit SA location information as part of its mapping functionality.

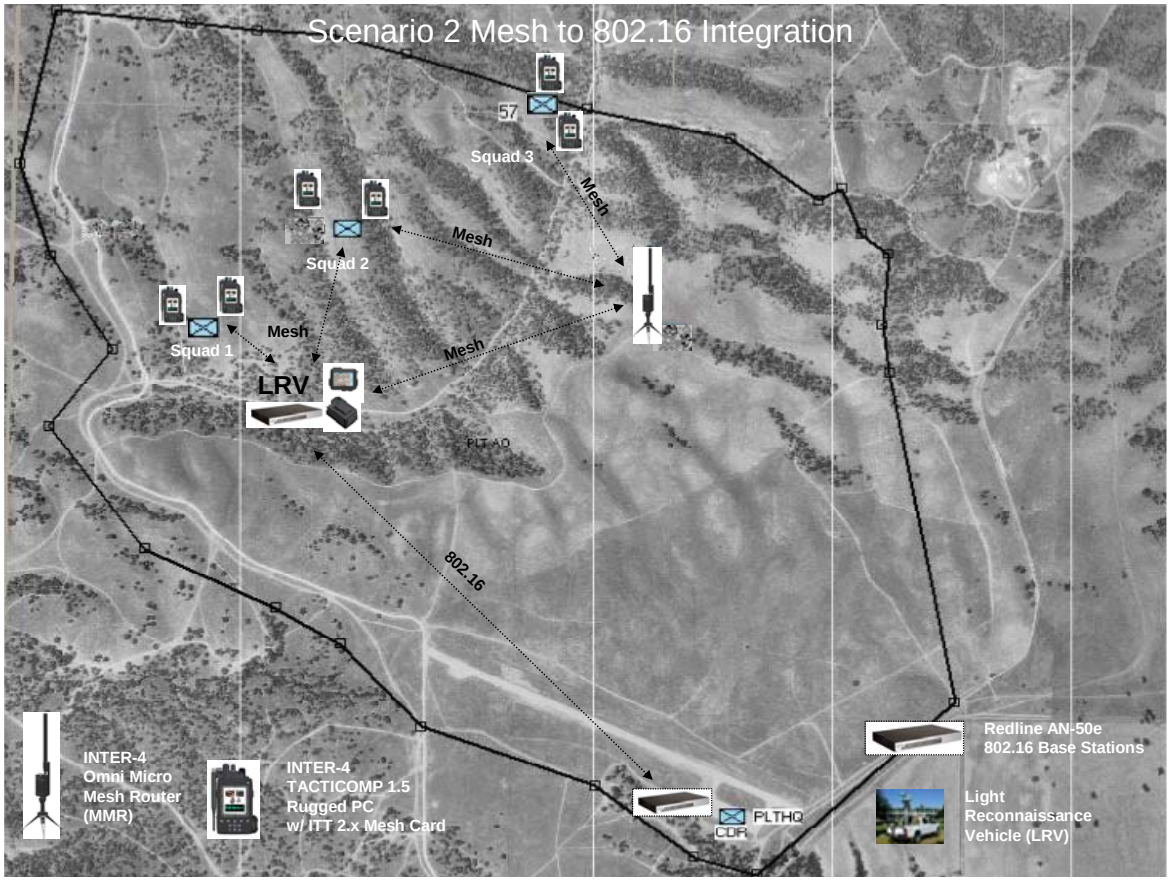

Figure 28. Scenario Two Access Layer/Battlefield Backbone Integration

Again during scenario two the ability to provide VOIP, text chat, streaming video, and SA data was tested, but over greater distances and greater dispersion between the meshed squads. The graphic in Figure 29, taken from the T-6 located in the TOC, shows the distances between nodes. Squad 3 extended its range the furthest from the LRV, maintaining network connectivity and full functionality as their distance form the LRV neared 3.5 kilometers in LOS and near LOS conditions.

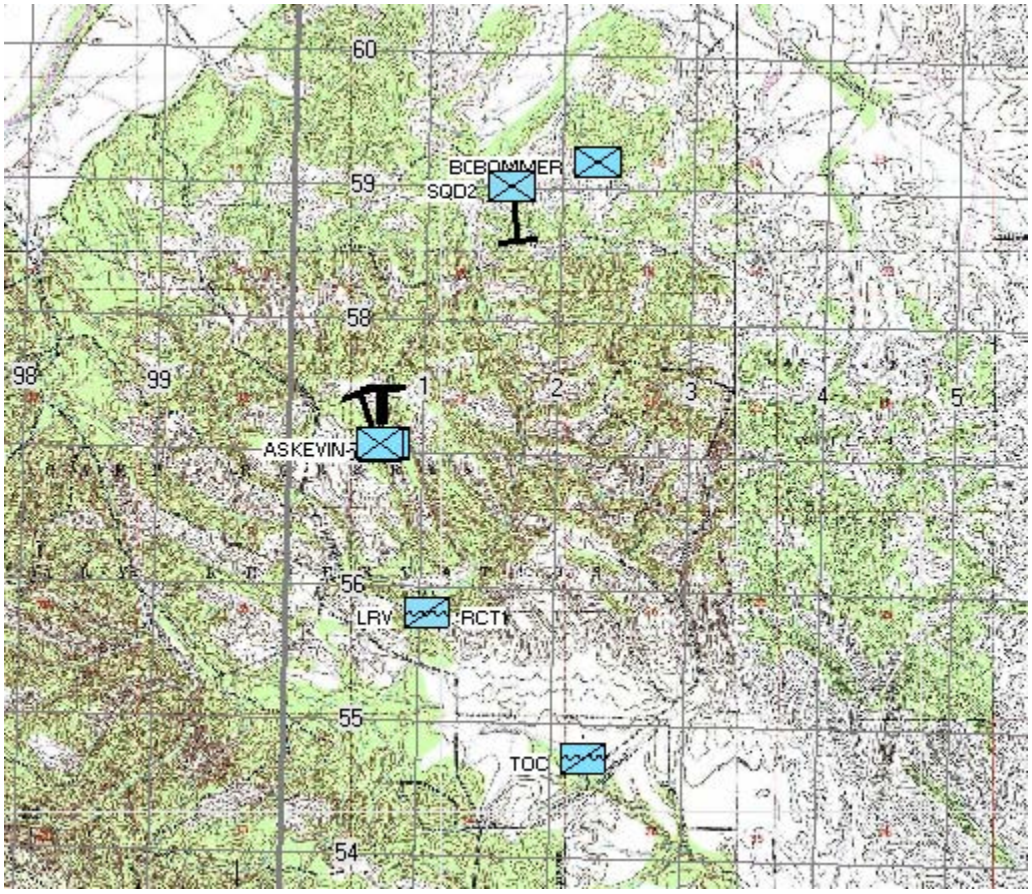

Figure 29. Scenario Two SA Graphic Depicting Extended Range

For the streaming video test, two additional video cameras were provided to squads 1 and 2. This portion of testing would evaluate the network's ability to successfully transmit multiple streaming video feeds at the same time to the same location, that being the TOC. The TOC successfully captured three concurrent streaming video transmissions from the squads, with an average frame rate of 7.5 frames per second. Figure 30 highlights the view from the TOC.

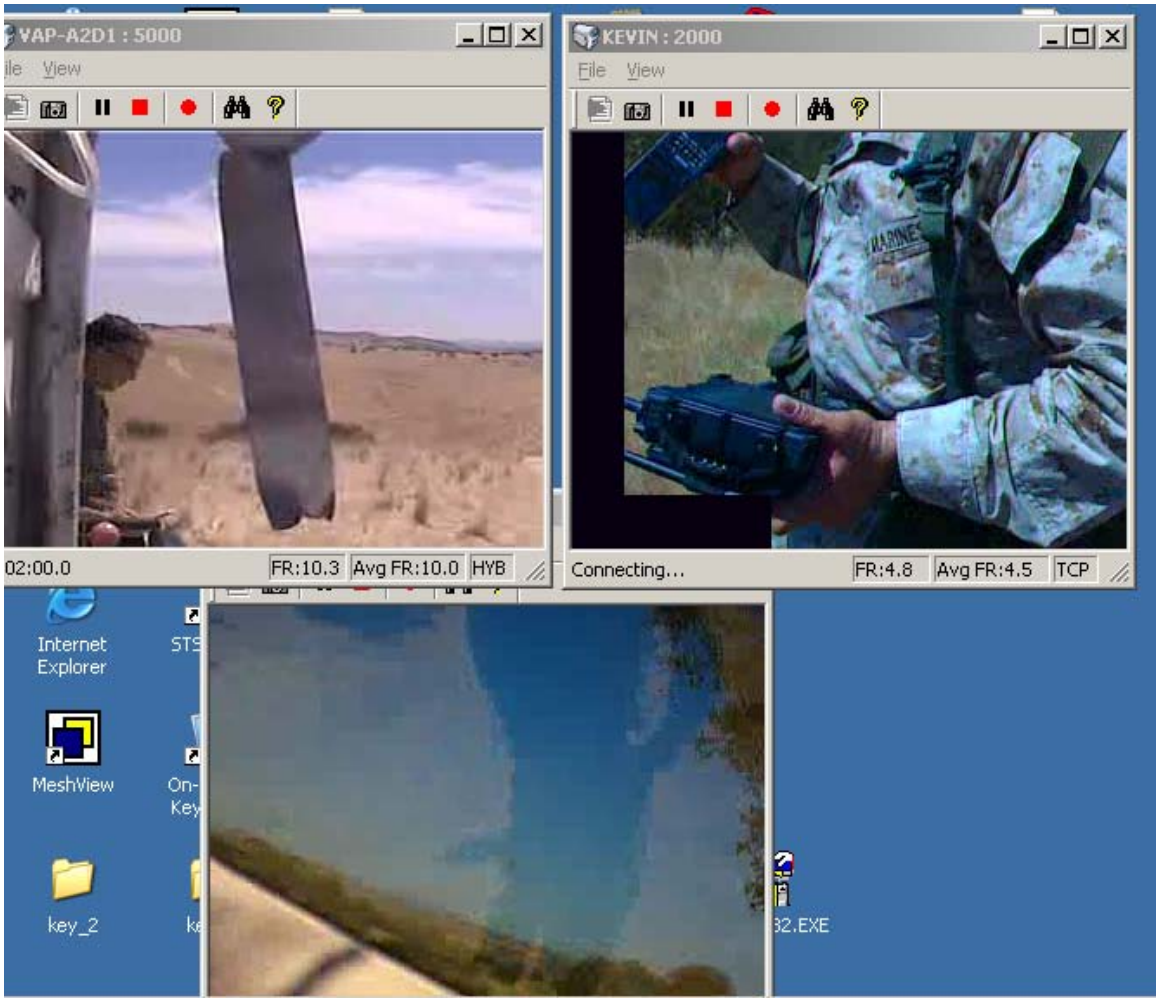

Figure 30. Concurrent Streaming Video as viewed from the TOC

Limited throughput testing was successfully executed due to the configuration issues that existed between the VAP and IXChariot. However the 802.16 link remained available for testing, and several throughput tests were performed over this link between the TOC and the LRV. Figure 31 provides a sampling of one of the tests, with the results displaying average throughput readings of 35 Mbps. In contrast, expected throughput of a SINCGARS transmission in similar situations would only result in 1.7 kbps.[16]

[16] See Table 1 for SINCGARS effective throughput analysis. In addition, SINCGARS lacks the ability to transmit in a point to multipoint configuration.

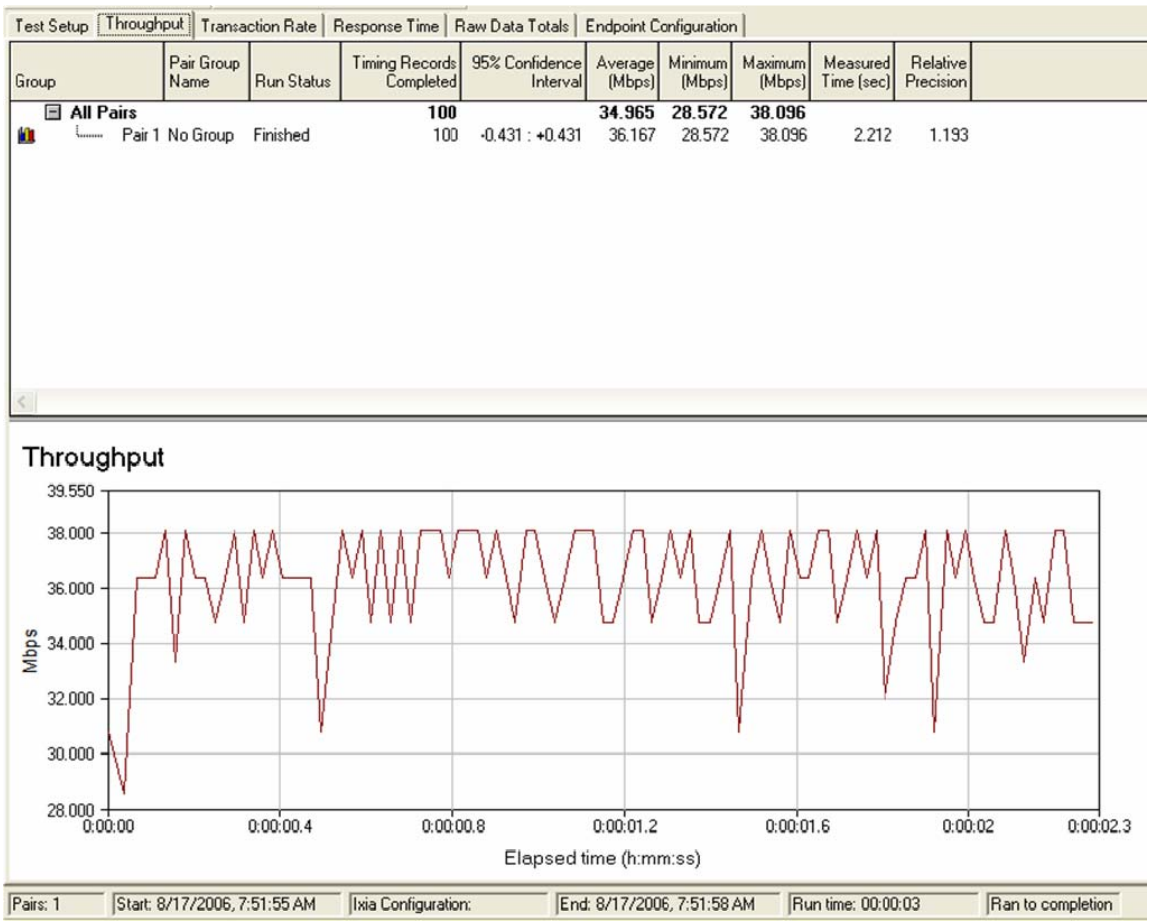

Figure 31. TOC to LRV 802.16 Battlefield Backbone

Scenario two demonstrated the capability to wirelessly transmit streaming video and PLI from the tactical level mesh over 100 miles via an 802.16 broadband link. This long-range connectivity was established through an existing wireless 802.16 network that links Camp Roberts and NPS (see Figure 32).

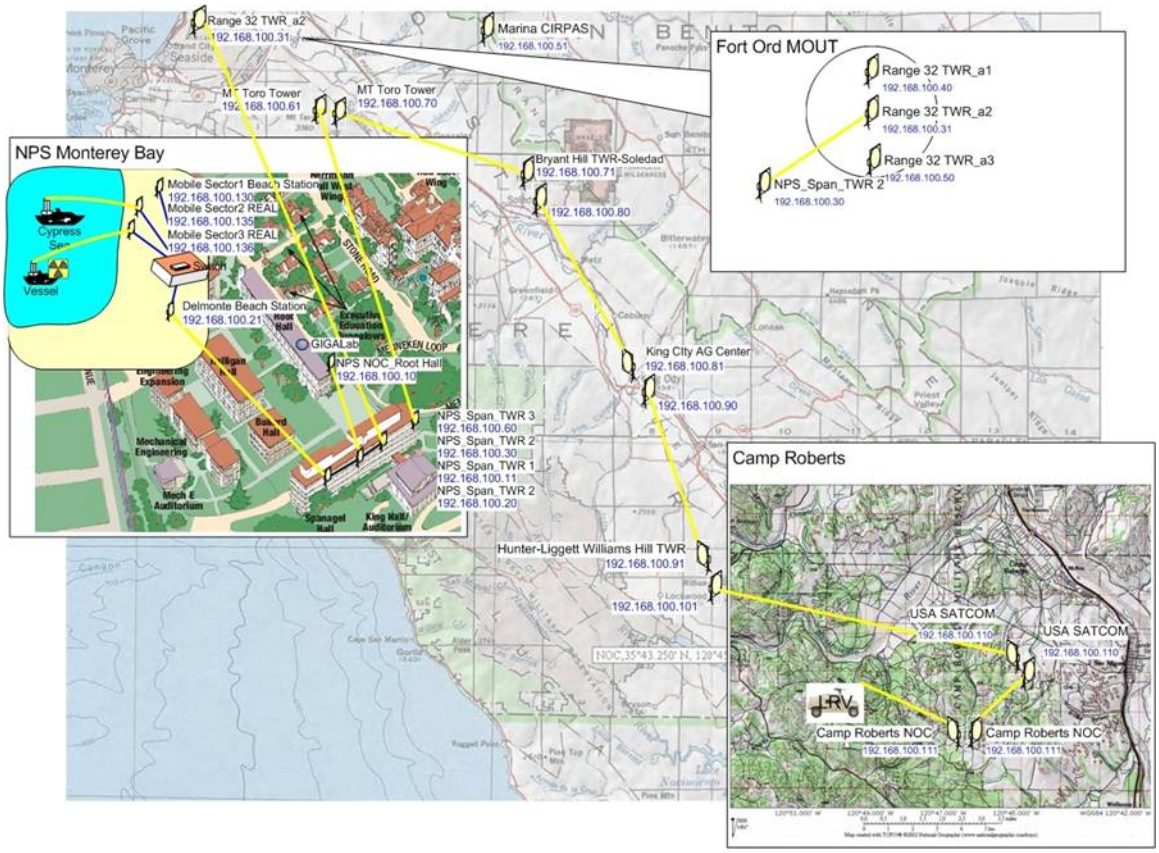

Figure 32. NPS – Camp Roberts 802.16 Network

The SA graphic highlighted in Figure 33 was captured in NPS's Global Information Grid Applications (GIGA) Lab during a brief which was conducted from Camp Roberts by the authors. The brief was presented to NPS staff and Boeing representatives attending an NPS sponsored Technology Expo.

Figure 33. SA Graphical Display as Viewed from NPS

6. TNT Field Experiment 06-4 Summary

These two scenarios conducted during TNT 06-4 validated our assumptions that a wireless meshed network can effectively serve as the access layer for DO units and that an 802.16 broadband link can reliably function as the battlefield backbone in support of tactical DO missions. Together, these two emerging technologies possess the ability to provide command and control to DO units with a capability several orders of magnitude above what the current communications architecture can support.[17] Throughout the duration of these experimentations, both the INTER-4 Tacti-Net product line and the Redline series of 802.16 radios successfully accomplished their respective missions in extending the tactical internet to reach DO units. Some equipment shortcomings were made apparent during the conduct of this research. Current form factors for the rugged PDAs tested remain less than ideal in tactical situations due to their bulk and dependence on the operators having to carry the device by hand. Future iterations should evolve into a wearable device with remote weapons-mountable operating controls.

[17] Refer to Table 1 on page 10 for a comparison of throughput performance to that of SINCGARS and EPLRS. Wireless mesh access layer throughput observed during testing averaged 650 kbps (See Figures 23 and 24), while the Redline 802.16 battlefield backbone throughput averaged 35 Mbps (See Figure 29).

THIS PAGE INTENTIONALLY LEFT BLANK

VI. DO ARCHITECTURE CONSIDERATIONS

The technologies evaluated during the Camp Roberts experiments, though promising, demonstrate that further research and testing is required before this conceptual architecture can be applied to Distributed Operations (DO) Forces writ large. Extending the tactical internet has the potential to distribute the shared situational awareness and enhance communications, which, if used correctly, will enhance the capabilities of the DO units.

It should be noted, however, that the Camp Roberts tests focused on a small scale mesh network combined with a battlefield backbone connection for longer range connectivity. This mesh network only forwarded information at the data link layer (layer 2) and did not include any network layer (layer 3) device routing. More detailed research will be needed as the number of mesh networks increase, specifically focusing on the appropriate layer 3 protocols that maintain route information as mobile nodes move throughout the battlefield.[18]

This chapter will provide recommendations to be used as a guide to evaluate desired system attributes for a DO network architecture. Further tests should evaluate technology against the system requirements detailed in this chapter. The recommendations in this chapter will not endorse a specific vendor or end system, but instead will focus on general system requirements to support both a platoon to higher headquarters battlefield backbone, as well as a platoon level mesh (or network access layer) that can adequately support the DO concept. All of the recommendations will be evaluated in reference to the Open Systems Interconnection (OSI) model.

A. PROPOSED SYSTEM ATTRIBUTES

1. General System Capabilities

The vision for extending the tactical internet to DO units centers on creating a network that provides an enhanced communications capability for the warfighters. This chapter will focus on the requirements to build a stable and robust network that can be used for any foreseeable purpose. The intent is to build a network where any application

[18] Specific recommendations for further research on this topic are detailed in Chapter VII.

can be used as a tool for DO units. For instance, a properly constructed network should be capable of supporting voice, video, position location, chat, and imagery capabilities across the network regardless of the application program. These applications can be incorporated throughout the warfighting functions, particularly in support of operational reporting, logistics, intelligence, and fire support. Creating one network that can be used for multiple purposes remains the focus.

Another point to consider when extending the tactical internet in support of DO units is that most solutions usually entail giving the Marines more equipment that increases their load. In this scenario, the end system should support multiple applications incorporated into one device. For instance, the end system should have the capability to run video, voice, position location, and chat message software, similar to the applications built into the INTER-4 product line. This device is then connected to the tactical internet where information from various applications can be sent and received. The solution should utilize the fundamentals of the internet (described later in this chapter) that enable almost any application program to transmit and receive data.

2. Networked Information Systems

In the past, the military has procured communication systems that have been, in essence, stovepipe solutions. These systems, as the name implies, are isolated systems that are not capable of integrating with other systems and cannot easily share information across a network. In many instances, these communication systems were developed with proprietary technology that was utilized only for that particular system. For instance, military single channel radio platforms cannot be incorporated into a network to share battlefield information. This practice needs to evolve and future technology should be developed using the Open Systems Interconnection (OSI) model as a guide. The goal is to design IP-based end systems that can be easily integrated into the battlefield internet.

3. Management

Network management software is required for the network to function efficiently in large scale applications. In a network with many nodes, problems are bound to arise that the users cannot repair on their own. A software based management protocol is needed to restore the nodes so that the users can focus on their primary task: warfighting.

This application will have the ability to query nodes on the network for node-specific information. Information about connection status, percentage of dropped packets, data throughput, etc., can be gathered from the network nodes where this information is utilized to make management decisions. The system should also be capable of automatically receiving information from nodes when there is a problem. It is recommended that the management system be located above the company level, in a location that is outside of direct enemy fire, and preferably reside at the battalion headquarters. This system can be deployed to monitor the network with the ability to resolve problems within the network.

4. Security

Security is another important consideration for units operating in a military environment. This is a very complex subject and could be a thesis topic by itself. At the very least, the data exchanged between DO units will be at the SECRET level (information concerning friendly/enemy location, intelligence material, and logistics requests will be some of the information that traverses this network). For that reason, measures must be taken to secure the data exchanged between units. There are numerous ways to secure the communications links. It can be secured at the physical layer, the network layer, and at the application layer. The ultimate goal of securing information is to enable end-to-end security, meaning that only the sender and receiver can view the data. Regardless of the security methods employed, they need to conform to the National Security Agency's (NSA) guidelines for securing information outlined in FIPS-140-2. Another important consideration in a mesh environment is securing the layer 2 and 3 link-state information. A reliable order of battle can be deciphered from the Address Resolution Protocol (ARP) or routing tables. This information should also be secured.

5. Layer 3, Network Layer Integration

a. Internet Protocol (IP) Based Applications

IP is the language of the Internet and has enabled a multitude of applications to transmit data seamlessly, for the most part, around the world. By using this protocol in a mesh environment, nodes will not only have the ability to transmit and receive information within their own local area network (LAN), but will possess the ability to access information from other sources around the world. Conversely, the

information that is generated at the platoon level can now be shared at the highest echelons for a more thorough Common Operational Picture. The goal of extending the tactical internet to the fireteam level is achievable largely due to the application of the IP protocol.

b. Multicast Capable

Most applications that utilize the internet employ uni-cast IP addressing to send and receive information. An example of uni-cast is node A addressing a packet destined for node B by using node B's IP address. For some applications a node may require the capability to send information to multiple nodes on the network. Instead of individually addressing every node, the transmitting node uses one multicast address to send the information to multiple nodes (multicast is described more thoroughly in Chapter III). In order for a node to receive the information destined for a multicast address, it must subscribe to this multicast address. The network protocol will manage multicast addressing and share this information map with all nodes in the network.

In a military environment, much of the data from both inside and outside the LAN will need to be shared amongst multiple nodes. Multicast makes this process much simpler and more efficient. In the DO scenario, multicast is more important for the mesh (or access layer) devices than for the battlefield backbone. The reason for this is that there may be multiple mesh nodes operating in a small geographical area while sharing limited data throughput. Finally, the multicast capability should exist at both the network layer and at the data link layer (a multicast IP address and a multicast MAC address). This is the case since node addressing occurs at both layers—inefficiency arises when the network layer uses a multicast IP address for multiple nodes and the data link layer uses a unicast media access control (MAC) address for an individual node. Layer 2 multicasting is possible, but it is still evolving as a capability in layer 2 protocols.

c. Stable Protocols for Ad-Hoc Environments

DO units will operate in a dynamic environment with units moving in and out of radio frequency (RF) range of the radio nodes. Consequently, there must be a stable mobile ad-hoc network (MANET) protocol that can maintain a current map of the network. This protocol is used to inform the network of changes and must do so without

degrading network performance by transmitting too many control messages. The Internet Engineering Task Force has sponsored a working group that is developing protocols that can be used in mesh networks. Another agency that is working with in subject area is the Defense Advanced Research Projects Agency (DARPA), who recently awarded an 18 month contract worth $7.8 million to BAE Systems, Inc.[19]

The process of distributing a current network map to all nodes in the network is called convergence. In simple terms, network convergence is the amount of time it takes for every node to receive updates of changes in the network. There are two methodologies that can be used for this purpose. One is to use a proactive protocol. A proactive protocol constantly probes the network for changes. Convergence in this protocol is usually faster, but at the price of increased network traffic. The second type is a reactive protocol. This protocol only transmits network updates when a node cannot be reached using information from the current routing table. Convergence is slower with this method when compared to the proactive protocol but produces less network traffic.[20]

Another key consideration for large-scale mesh employments is the level where routers are employed. The thesis experiments at Camp Roberts were designed around layer 2 devices that did not perform layer 3 routing. If mesh networks are ever employed at the regimental or division level, then stable MANET routing protocols must be used. The integration of multiple mesh networks into the SIPRNET will necessitate the use of layer 3 routing.

d. Connection Prioritization

In any network, various metrics are used to determine the best path to get from one point in a network to another. In older protocols only metrics like hop-count (how many networked devices are traversed during network transit) were used to make a best-path determination. In a mesh network, however, multiple metrics should be used to determine the best path. Metrics include data rate, RF signal strength, percentage of

[19] See "DARPA Awards Tactical Network Deal" by Doug Beizer in Government Computer News at http://www.gcn.com/online/vol1_no1/41388-1.html (September 2006)

[20] Convergence and MANET protocols are described in further detail in Chapter III.

dropped packets, traffic load, etc., should be utilized to determine the most efficient paths in the network. With this information, the network can maximize the organic data throughput and operate more efficiently.

6. Layer 2, Data Link Layer

a. Stable MAC Layer

At the second layer in the OSI model, the MAC functions are extremely important for the proper functioning of a mesh network. The functionality of this layer must provide for the proper transmission of appropriate control messages that manage the network. In addition, this management must occur while operating in a dynamic environment. This layer will broadcast the scheduling assignments for the nodes in the networks which make data management more efficient. This layer will also have the ability to adjust to changes in network topology (as nodes move on the battlefield) and will distribute this updated information to the network (Chapter III described this process in greater detail). The MAC layer needs to be robust and capable of handling the aforementioned processes even as the network increases in size, otherwise the network will collapse. For this reason, contention based access methods (like Carrier Sense Multiple Access) should not be used in this context.

b. Quality of Service (QoS)

QoS capability is important in any networked environment, specifically in a dynamic military mesh environment. As described in Chapter III, certain types of traffic should be given priority during network transit. Real time traffic like streaming video, video teleconferencing, and voice over IP (VOIP) need higher prioritization than does standard network traffic, otherwise these applications can be adversely affected. Priority scheduling is not the only reason to use QoS. QoS also provides a method to manage limited data throughput, and make more efficient use of this limited resource. This is particularly true at the mesh layer where shared data rates are significantly less than the battlefield backbone's data rate.

c. Node Authentication Prior to Network Entry

Prior to entering a network, node authentication should take place to ensure that only authorized nodes can utilize network resources. The logic behind this is obvious for military applications. There are promising technologies that can be used to

authenticate users to the network. Digital certificates, Public Key Infrastructure (PKI), and biometrics technology show potential and are means to authenticate users to the network.

d. Layer 2/3 Interface

Networks are comprised of many different layer 2 technologies like Ethernet (802.3) and Wi-Fi (802.11), for example. Despite their differences at the MAC level, these technologies are capable of communicating with other nodes even when they are attached to separate LANs that use different layer 2 protocols. Most layer 2 technologies use the 802.2 Logical Link Control layer protocol, which provides a standardized interface between the data link layer and the network layer. The use of this interface makes a protocol both bridgeable and routable. Independent of a specific interface, the end requirement is to provide a routable network comprised of disparate modules that can be attached to any portion of the network and still function.

7. Layer 1, Physical (PHY) Layer

a. Frequency Range

The frequency ranges used today in many commercial devices is for U.S. civilian use and is in the Industrial, Scientific, and Medical (ISM) bands and is centered at 900 MHz, 2.4 GHz, and 5.8 GHz. The Europeans have a similar band and is in the 800 MHz band. In order to avoid any conflicts with these widely used commercial bands, another frequency range should be used; otherwise the network could be diminished because of too many devices utilizing the same frequency. For instance, the frequency shifted INTER-4 Tacticomps operate at 2.X GHz and the Redline AN-50's operate between 5.470-5.725 GHz and between 5.725-5.850 GHz. Care should be taken when selecting frequencies to avoid conflict with the many civilian frequency bands used worldwide. In addition, adjusting the radio frequency to other ranges can also improve a device's capability to penetrate foliage and other battlefield impediments.

b. RF Propagation for Mobile Nodes

One of the requirements for connectivity in a dynamic and mobile environment is the ability for a device to manage Doppler shifted radio frequencies. When an RF node is transmitting while on-the-move (OTM), the transmitted radio frequency will be shifted either to the right or left (shifted to a higher or lower frequency)

depending on the direction of movement compared with a stationary node. The networked radio system must be capable of adjusting to this frequency shift in order to properly receive the transmitted data.

c. Low Probability of Interception/Low Probability of Detection (LPI/LPD)

In a military environment LPI/LPD is an important concern. Both the battlefield backbone and mesh (or network access) layers should be designed with LPI/LPD technologies. Frequency Hopping and Direct Sequence Spread Spectrum are technologies that can be applied to limit enemy detection.

B. REQUIREMENTS FOR PLATOON/COMPANY LEVEL BATTLEFIELD BACKBONE

1. Employment

Figure 34 illustrates the concept of battlefield backbone. Both the platoon and company headquarters require the ability to transmit information over long distances. Without these connections, the companies are, in essence, isolated from the tactical internet. Currently, the DO units' only connection to higher headquarters is via voice-only radios. In the example scenario, both the platoon and company headquarters will bridge their local mesh traffic into a backbone link for long range connections. The reach-back enhances situational awareness at all levels and provides lower level units with the ability to connect into the Secure IP Router Network (SIPRNET) cloud. The Redline AN-50 radios were used as the battlefield backbone connection in the Camp Roberts experiments and are described in Chapter IV (on a side note, the Redline AN-50 radios are currently being utilized in Iraq for long range, fixed connectivity).

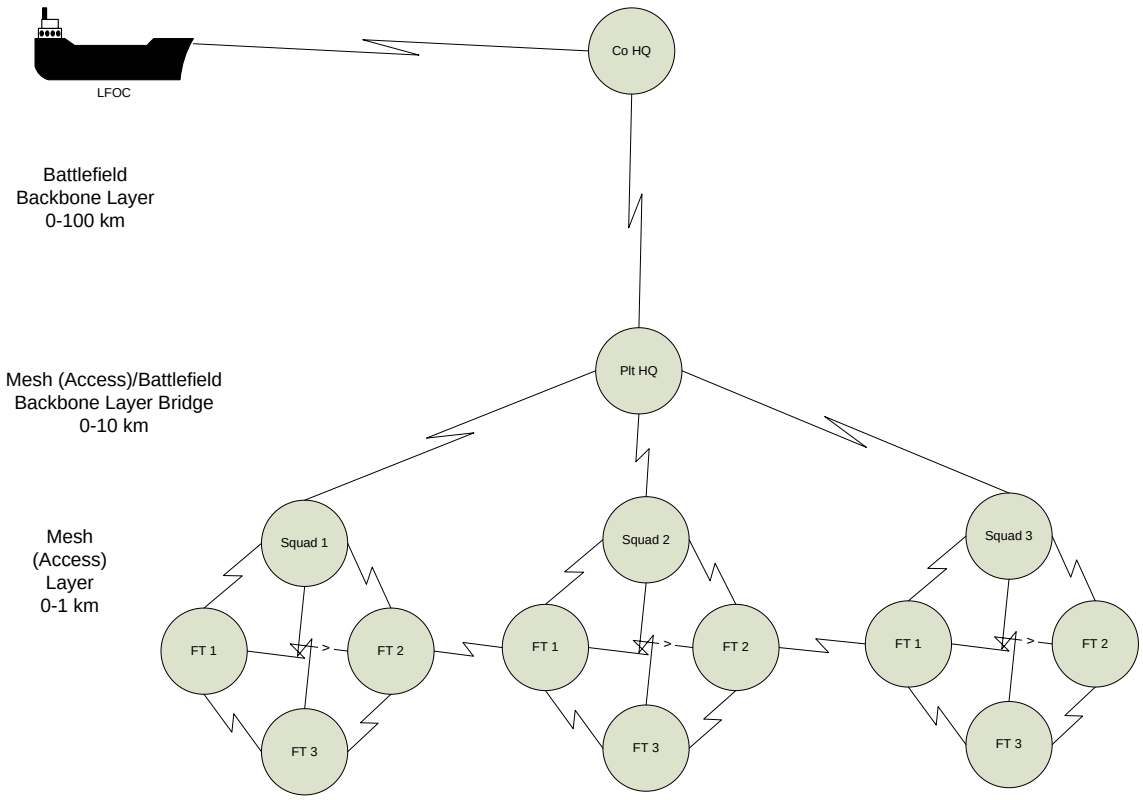

Figure 34. Conceptual DO Communications Architecture

Although Figure 34 does not depict it, there will be three platoons with long range connections to the company headquarters. This necessitates the need to connect the radios in a point-to-multipoint mode (PtMtp).[21] In this scenario, all connections remain fixed in location and non-mobile. The inability to communicate OTM to higher headquarters via a battlefield backbone connection is a liability. In a perfect world, the platoons would be capable of maintaining their connections to higher headquarters while OTM. At this point in time, however, no long range high data rate radios exist that can support OTM communications.

Figure 34 also highlights the fact that the platoon to company link represents a single point of failure. A better scenario, which is shown in Figure 35, would be for the three platoons and the company headquarters to connect into a mesh network instead of a PtMtp connection. A mesh connection would provide more flexibility for all of the nodes

[21] Point-to-multipoint was described further in detail in Chapter III.

and would eliminate the single point of failure problem associated with PtMpt connections. As long as the nodes were within radio frequency range of another node, they have the ability to connect to the tactical internet. Similar to the OTM concept, there are no long range, high data rate radios that operate in a mesh mode. The IEEE 802.16-2004 standard does include extensions for mesh connectivity, and this technology shows promise for building mesh networks in the future.

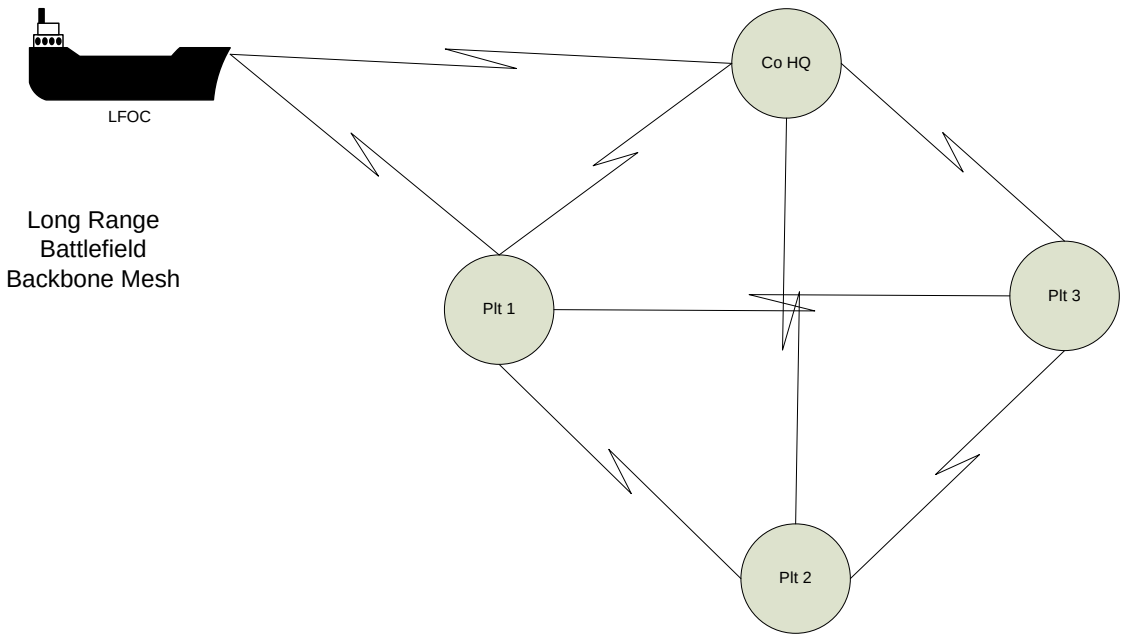

Figure 35. Conceptual DO Battlefield Backbone Mesh

2. Range/Antenna Requirements

The distance required for the battlefield backbone links from the platoon or company headquarters need to extend up to 100 kilometers. The extended range necessitates the use of advanced antenna technologies that can transmit long distances. Highly directional antennae are essential for this purpose. Since at least one of the nodes will operate in a point-to-multipoint manner (the company headquarters), antenna arrays should be utilized in order to receive the signals from nodes which are unevenly distributed on the battlefield.

3. Form Factors

There are three types of form factors required for backbone employment. The first form factor is for dismounted troops. The radio should be small and light enough to fit inside a military issue backpack and be carried by one Marine. The antenna should also be compact so that it can be easily folded up and transported by one Marine, while no more than two Marines should be required to erect and align it. Antenna type remains an important consideration. An omni-directional antenna is easier to operate (no pointing), but has less range. Another option is a directional antenna which has greater range but must be aimed at the distant station.

The second form factor applies to radio-mounted HMMWV platforms. This radio will be powered from the vehicle batteries. The antenna will be mounted to the vehicle and can be easily erected, aimed, and stabilized by one Marine. Omni-directional or directional antenna types are a consideration here as well. One more factor to be considered is that the antennas and radios meet military specifications.

The third form factor involves the employment of radios in an aerial platform such as an Unmanned Aerial Vehicle (UAV), a balloon, or in manned aircraft. This configuration type would greatly extend network connectivity across NLOS conditions, such as in rugged mountainous terrain and built-up urban environments. Weight factors and power requirements will also be key considerations for this type of application.

4. Power Requirements

The man-portable radio described above will be powered by a transportable DC battery source. Current military batteries like the 12 volt BA-5590 should be used to provide power for the radio. Battery life for these radios should be between 12-24 hours. As stated above, the vehicle mounted radio can be connected to the vehicle batteries that can provide uninterrupted DC power.[22]

5. Data Throughput

The actual requirement for data throughput at this level is unknown. Baseline devices like the Aeronix IEEE 802.16-2004 radios and the Redline AN-50 should be used as a comparison. Aeronix claims data rates of 70 Mbps at a distance of 70 miles.

[22] Solar energy may provide an additional source of power that may warrant further investigation.

C. REQUIREMENTS FOR PLATOON LEVEL MESH (ACCESS LAYER)

1. Employment

Figure 34 illustrates the mesh architecture for DO units. The platoon mesh consists of at least 13 nodes (four per squad times 3 squads plus the platoon headquarters). Each of these mesh devices share the network and have the ability to send and receive voice, video, imagery, chat, and situational awareness traffic. The mesh network is self-forming and self-healing. This allows the devices to move about the local battlefield and still maintain connectivity as long as they are within range of another mesh node. The mesh devices also provide true OTM capability. As outlined in Chapter IV, at the Camp Roberts experiments the platoon level nodes form a mesh network using INTER-4's Tacticomp devices. This nomadic layer-2 mesh characteristic can present challenges when routers are introduced into this architecture. Further research is required to address battlefield mobility and seamless network coverage.

2. Range/Antenna Requirements

The range for the mesh devices should be at least 1 kilometer. The devices will utilize an omni-directional antenna to provide connectivity to the mesh network.

3. Form Factor

INTER-4's Tacticomp 1.5 is a baseline form factor for a ruggedized mesh network device. The Tacticomp dimensions are: 7. 75" x 3.25" x 2" and weighs just over two pounds. The device can be easily held with one hand and can fit inside a cargo pocket. The visual display is large enough to view map graphics, imagery, and video. INTER-4 has designed various carrying options for the device when not being held in the hand. It can be secured on a ballistic vest or strapped on the forearm. The device meets the MIL-STD-810F that complies with military environmental standards.

4. Power Requirements

The mesh radio device will operate independent of a vehicle and will be powered by a replaceable DC power source. The radio should operate on one battery for a period of 14-24 hours depending on usage. As a baseline, the INTER-4 Tacticomp can operate on one battery for a range of 14-24 hours depending on device use.

5. Data Throughput

The ITT MEA card embedded in the INTER-4 Tacticomp is the baseline for data throughput. The data throughput for this device is a shared network throughput of 2 Mbps, and 6 Mbps in burst mode. Obviously as the number of nodes in the network increases, the less throughput is allotted per node.

D. SUMMARY

Constructing a solution to extend the tactical internet for DO units is challenging but achievable. Currently, there are available technologies that can be assembled to form a solution and build a network that can be used by DO units to send/receive video, VOIP, imagery, situational awareness traffic, and chat traffic. The technologies continue to rapidly evolve and further product research and evaluation is recommended. Technologies like MEA mesh, IEEE 802.16-2004, IEEE 802.16e should be evaluated against the requirements specified in this chapter. Companies such as Intel, Aeronix, INTER-4, and Redline are active in this area of research and their products show promise. These vendors' products should be further evaluated and tested. After further research, testing, and refinement, a robust and dependable mesh network can be developed for DO units. The final recommendations will be described in the next chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION AND RECOMMENDATIONS FOR FURTHER RESEARCH

A. CONCLUSION

This thesis focused on the topic of how to extend the tactical internet to reach Distributed Operations (DO) units. DO presents many interesting and dynamic challenges. These units will operate independently in austere environments separated from many of the support functions in which Marine Corps infantry units now operate. The challenge from the communications perspective is how to bridge the so-called last tactical mile, so that leaders at the platoon level and below can take advantage of the tactical internet to distribute and consume battlefield information.

The Marine Corps Warfighting Lab (MCWL) is currently developing the doctrine, tactics, techniques, and procedures for these units. In defining this concept, MCWL has also identified a tentative Table of Equipment (T/E) capable of supporting DO units. The communications portion of the T/E, while well thought out, does not provide DO units with the ability to exchange real-time PLI updates, streaming video, digital imagery, or chat messaging. The T/E simply uses current military radios that only provide the capability to exchange voice traffic and limited digital information. This thesis proposed an alternative network-based DO communications architecture, and demonstrated the feasibility of equipping a DO platoon with a tactical wireless mesh and long haul capability.

Various network architectures were tested in a simulated DO environment during the Camp Roberts' experiments. The first scenario tested the platoon level and below mesh or access layer, while the second scenario simulated bridging the meshed network across a terrestrial battlefield backbone connection from the platoon level to higher headquarters. The topography of Camp Roberts provided varied terrain for tests in both line-of-sight and non-line-of sight scenarios.

The initial assessment demonstrates that a tactical wireless mesh network combined with a battlefield backbone connection is feasible and has the potential to support a DO-sized unit. Many tests were conducted in the mesh scenario and different

application programs were used to demonstrate that mesh networks could be used to send and receive voice over internet protocol (VOIP) traffic, streaming video, position location information, and chat message traffic across this platoon-sized mesh network. The tests demonstrated that this technology, at least in an experimental environment, could be used to extend the tactical internet to the platoon level.

The second scenario built upon the first by successfully demonstrating the use of the IEEE 802.16 technology in establishing a battlefield backbone that provided the connectivity between the meshed network of DO squads and platoon headquarters to the company headquarters. These connections are vital for the DO platoons since they will be geographically separated (outside the range of current mesh network devices) and will require the long-haul communication capability to exchange information across the battlefield. The results of the experimentation demonstrated that platoon level mesh nodes could exchange information through the mesh/802.16 bridge (Redline AN-50e radios located in the Light Reconnaissance Vehicle (LRV)) to a simulated higher headquarters. This information consisted of VOIP traffic, streaming video, position location information, and chat message traffic. The highlight of the experiments came when streaming video was transmitted from an encrypted mesh node 100 miles over an 802.16 link from Camp Roberts to the Naval Postgraduate School in Monterey.

B. RECOMMENDATIONS FOR FURTHER RESEARCH

Although the experiments supporting this thesis showed promise, additional research and testing is required to determine a wireless network solution that is compatible with the DO concept of employment. The authors recommend that a network architecture be constructed based upon a platoon level mesh network that is connected to higher headquarters via a long range, IP-addressable radio (battlefield backbone) connection. Further research should focus on the following:

1. Mesh Scalability

The Camp Roberts experiments showed that mesh technology can be implemented at the platoon level, but further research is required to identify potential network scalability issues as mesh networks expand to support the spectrum of communications spanning the company through division level. As the number of nodes

expands in a single mesh network, network control messages will increase. Network management, therefore, will become more complex and network throughput will diminish. This necessitates identifying the maximum number of nodes that can operate effectively in a single mesh network.

As mesh networks begin to proliferate on the battlefield, maintaining node location information will become difficult.[23] Convergence of the network in a large-scale mesh environment becomes complicated when nodes move between geographically separated mesh networks operating in the battlespace. Further research should identify appropriate layer 3 routing protocols and potential employment scenarios (company, battalion, regiment, UAVs, etc.)[24] Additionally, autonomous system designation remains vital for proper network functionality. Critical factors in supporting mesh scalability include the appropriate routing protocol selection and identifying their key employment locations within the network architecture.

2. Mesh Interoperability with Current Tactical Backbone

Compatibility between mesh networks and the current SIPRNET backbone is another area requiring research. If mesh networks at the platoon level become the norm, problems may arise when connecting these mesh networks to the SIPRNET backbone. An increase in network traffic across this backbone may impose significant throughput restrictions due to an increase in data throughput requirements.

3. Mesh and Battlefield Backbone Technologies

Emergent Mesh and battlefield backbone technologies should continue to be evaluated in order to assess their potential for integration into the DO wireless network. Additional research should include: next-generation INTER-4 and ITT mesh systems and devices, IEEE 802.16e standards-based devices which promise mesh-like capabilities, and IEEE 802.16-2004 standards-based radios for battlefield backbone communications.[25]

---

[23] In this instance, node location information refers to the network path a packet must travel to arrive at the given destination node.

[24] Bridging technologies have been intolerant of loops that arise with addition of redundant connection links. This redundancy is necessary for a meshed DO platoon. The behavior of various mesh technologies is unknown when the network grows in scale.

Further experiments should continue to leverage previous NPS thesis work and field research in order to advance the understanding in this relevant research area. An iterative approach, validated through field research and vendor collaboration, may prove the best course to achieving at least an 80% solution that DO units can utilize.

[25] Intel appears to be the leader in supporting and marketing IEEE 802.16e based technologies. For military specific application, Aeronix remains heavily involved in research and development of IEEE 802.16-2004 systems and products.

APPENDIX

A. IEEE 802.16 PRODUCT COMPARISON

The following chart provided by the U.S. Army Communications-Electronics Research, Development and Engineering Center (CERDEC), depicts the specification and performance characteristics of four prominent COTS vendors currently providing IEEE 802.16 broadband capabilities to the DoD in varying capacities. These four vendors; Orthogon Systems, Redline Communications, SMR, and BAE/Aeronix, either currently support wireless broadband services or are participating in current testing and evaluation to provide near-term support for one or more service branches within DoD.

	Orthogon Systems-Gemini	Redline AN-50e	SMR	BAE/Aeronix
RF Band	5.4 or 5.8 GHz	5.4 or 5.8 GHz	2.4 GHz	4.6 or 5.8 GHz
Channel Size	11 MHz	20 MHz	22 MHz	20 MHz
Available Channels	19	27	11	4.6 GHz – 9 5.8 GHz - 4
Max Simultaneously Usable Channels	10	7	3	4.6 GHz – 9 5.8 GHz - 4
Dynamic Channel Control	*Intelligent* Dynamic Frequency Selection	5.8GHz: Manual 5.4Mhz: Dynamic Freq Selection	Manual	Manual Automatic as part of Mesh MAC
Data Rate1	Up to 44Mbps	Up to 49Mbps	Up to 54 Mbps	Up to 65 Mbps
Receiver Sensitivity	-96 dBm (Adaptive)	-86 dBm (at 6Mbps)	-90 dBm	-90 dBm
Antenna Polarity	Dual2 (ODU has 2 int. ant; 1 vertical, one horizontal	Single (either vertical or horizontal)	Single (vertical)	N/A
Transmit Power	Up to 25 dBm (Adaptive) 316 mW	Up to 20 dBm (Adaptive) 100 mW	37 dBm 5 Watts1 (with Amplifier)	5.8 GHz – 2W (FCC Limit) 4.6 GHz - >100 Watts ERP
Standard Antenna Gain	23 dBi (14”)	PTP: 22 dBi (12”) PMP: 15 dBi (60 or 120o)	6 dBi Omni	N/A
EIRP2	18 dBW	PTP: 12 dBW PMP: 5 dBW	13 dBW	46 dBW @ 4.6 GHz
Maximum Range3	Up to 124 miles LOS	Up to 50 miles LOS	10 Miles LOS (Unclassified)	75 Miles LOS with 24 dBi dir antenna
Pt-to-MPt Capable	No	Yes	Yes	Yes
Operated OTM	No	No	Yes4	Yes5
Security/ Encryption	Proprietary Optional 128-bit AES	Proprietary	256-bit AES-CTR Pending NSA Type 1	Ext Type 1–ComSec 256bit AES-TranSec

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] Marine Corps Warfighting Lab. "Distributed Operations 2006 Capabilities and Enhancements Report." Internet: http://www.mcwl.usmc.mil/SV/DO%20CapEnhncRpt_19%20Jan%2005.pdf, July 17, 2006 [August 30, 2006]

[2] S. Lee. "Distributed Operations C4 Brief." Presentation, Marine Corps Warfighting Lab, Quantico, Virginia, 2006.

[3] United States Marine Corps. "A Concept for Distributed Operations." Internet: https://www.mccdc.usmc.mil/FeatureTopics/DO/A%20Concept%20for%20Distributed%20Operations%20-%20Final%20CMC%20signed%20co.pdf, July 17, 2006 [September 30, 2006].

[4] Congressional Budget Office. "The Army's Bandwidth Bottleneck." Internet: http://www.cbo.gov/showdoc.cfm?index=4500&sequence=2, [August 30, 2006]

[5] Held, Gilbert. *Wireless Mesh Networks*. Boca Raton, Florida: Auerbach Publications, 2005, p. 2.

[6] INTER-4 Product Information. Internet: http://www.inter-4.com/products/T15.html. [August 30, 2006]

[7] INTER-4 Product Information. Internet: http://www.inter-4.com/products/omniMMR.html. [August 30, 2006]

[8] Redline Communications Product Information. Internet: http://www.redlinecommunications.com/products/AN50e.html. [August 30, 2006]

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

Alberts, David, et al. *Network Centric Warfare: Developing and Leveraging Information Superiority*, Washington D.C.: CCRP Publication Series, February 2000.

Akyildiz, Ian F. *A Survey on Wireless Mesh Networks.* IEEE white paper [online] http://ieeexplore.ieee.org . Last accessed June 6, 2006.

Caceres, Francisco, and Swearingin, Brad. *An Analysis of IEEE.802.11b and 802.16 Technologies as Part of the Tactical Internet.* Master's Thesis. Naval Postgraduate School. September 2005.

Fu, Liqun, Cao, Ahigang and Fan, Pingyi, *Spatial Reuse in IEEE 802.16 Based Wireless Mesh Networks*. IEEE white paper {online} http://ieeexplore.ieee.org. Last accessed May 15, 2006.

Ghosh, Samik, et al. *What a Mesh! An Architecture for Next Generation Radio Access Networks.* IEEE white paper [online] http://ieeexplore.ieee.org. Last accessed May 15, 2006.

Guice, Robert, and Munoz, Raymond. *IEEE 802.16 Commercial Off the Shelf (COTS) Technologies as a Compliment to Ship to Objective Maneuver (STOM) Communications.* Master's Thesis. Naval Postgraduate School. September 2004.

Hall, Zygmunt J. and Hung-Yu Wei, et al, *Interference-Aware IEEE 802.16 WiMax Mesh Networks*. IEEE white paper {online} http://ieeexplore.ieee.org. Last accessed May 15, 2006.

Held, Gerald. *Wireless Mesh Networks.* Boca Raton, FL: Auerbach Publications, 2005.

Mylavarapu, Ramana, *Security Considerations for WiMAX-Based Converged Network*. White paper [online] at http://www.rfdesign.com. Last accessed May 15, 2006.

Olexa, Ron. *Implementing 802.11, 802.16, and 802.20 Wireless Networks: Planning, Troubleshooting, and Operations,* Burlington, MA: Elsevier Inc. 2004.

Sweeney, Daniel. *WiMax Operator's Manual: Building 802.16 Wireless Networks,* Berkeley, CA: Apress Publishing, 2004.

Vaidya, Nitin H. Class Lecture, Topic: "Mobile Ad Hoc Networks: Routing, MAC and Transport Issues." CS 4550, Computer Science Faculty, Naval Postgraduate School, March 2006.

WiMAX Forum. *Mobile WiMAX- Part I: A Technical Overview and Performance Evaluation*. [online] at http://www.wimaxforum.org. Last accessed June 6, 2006.

WiMAX Forum. *Mobile WiMAX- Part II: A Comparative Analysis.* [online] at http://www.wimaxforum.org. Last accessed June 6, 2006.

Wongthayarawat, Kitti. *IEEE 802.16 Based Last Mile Broadband Wireless Military Networks with Quality of Service Supports.* IEEE white paper [online] http://ieeexplore.ieee.org . Last accessed June 6, 2006.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education
   MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center,
   MCCDC, Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California

7. Dan Boger
   Naval Postgraduate School
   Monterey, California

8. Carl Oros
   Naval Postgraduate School
   Monterey, California

9. Rex Buddenberg
   Naval Postgraduate School
   Monterey, California

10. Marine Corps Warfighting Lab (Attn: C4)
    Quantico, Virginia